5

Networking

5.1 SNA – System Network Architecture

Die System Network Architecture ist ein Netzwerkverfahren, das Anfang der siebziger Jahre von IBM entwickelt wurde. Ziel war es, alle IBM-Systeme auf eine gemeinsame Netzwerkbasis zu stellen.

Das SNA verwendet eigene, im Rahmen der IBM-Welt standardisierte, Schnittstellen, Verfahren, Programme und Tools, die eine Systemverbindung zweier oder mehrerer IBM-EDV-Systeme ermöglichen. Wichtig dabei ist, daß es im Prinzip wenig relevant ist, ob dieses Systeme nun AS/400-, Mainframe- oder PC-Rechner sind. Die Adressierungsverfahren sind einheitlich und unterstützen somit eine relativ einfache Systemverbindung. Wichtig ist meines Erachtens, eine Einordnung und Definition von typischen SNA-Begriffen vorzunehmen, da diese und ihre Begrifflichkeiten oftmals falsch angewendet werden und letztendlich zum Mißerfolg einer Rechnerverbindung beitragen.

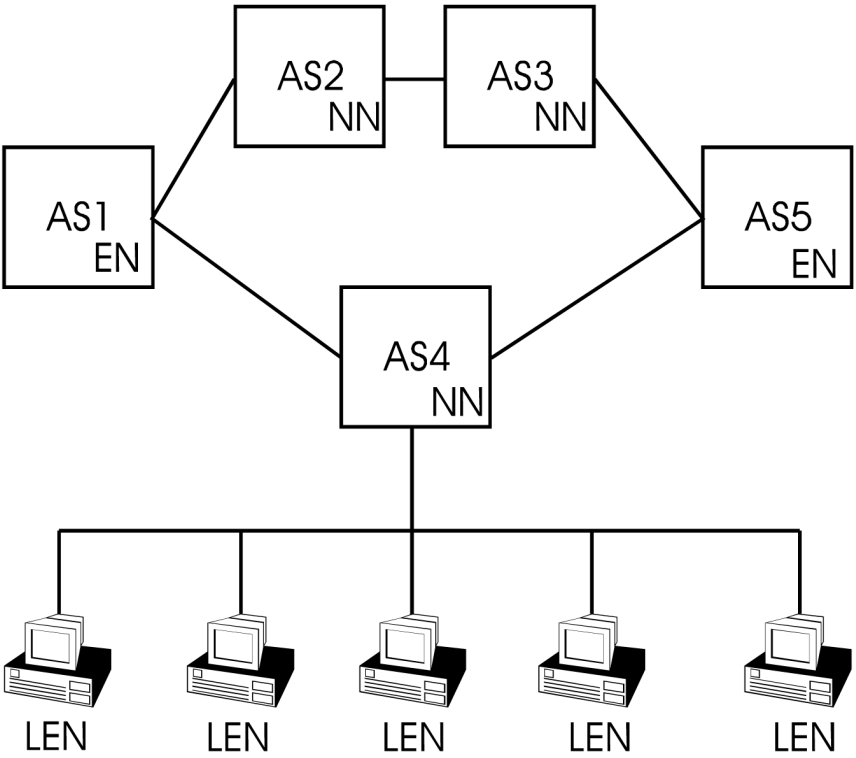
5.1.1 APPN – Advanced Programm to Programm Network

Die SNA unterscheidet grundsätzlich zwei unterschiedliche Netzwerkarchitekturen. Eines ist das, historisch ältere, APPC-Netzwerk. Diese Architektur ermöglicht die direkte Verbindung von zwei benachbarten Systemen und ist für komplexere Netzwerke nur schlecht einzusetzen.

Demgegenüber ermöglicht das APPN-fähige Netzwerk die Darstellung komplexerer Netzwerktopologien, so daß ein direkter Sitzungsaufbau zwischen nicht benachbarten Systemen erfolgen kann. Die Integration von PCs in die Dienste einer AS/400 ist im Rahmen von APPN-fähigen Netzwerken zu betrachten.

Wodurch zeichnet sich ein APPN-Netzwerk aus?

5.1.1.1 Knoten



Jedes System in einem SNA-Netzwerk wird als Knoten bezeichnet. Mit Hilfe des Knotens wird die Fähigkeit eines Systems im Netzwerk beschrieben.

Folgende Knoten werden unterschieden

NN = Netnode

Ein Netnode ist ein weiterleitungsfähiger Knoten im APPN-Netzwerk.

Gehen wir von folgendem Sachverhalt aus und betrachten obiges Bild: Es ist unsere Absicht, Daten von System AS1 nach AS5 zu senden. Da die Systeme AS2 und AS3 als Netnodes definiert sind, sind sie in der Lage, empfangene Daten weiterzuleiten, so daß letztendlich die Daten zum System AS5 gesendet und von diesem empfangen werden.

EN = Endnode

Ein Endnode ist ein nicht weiterleitungsfähiger Knoten im APPN-Netzwerk.

Betrachten wir wieder das Bild: Sollen jetzt Daten direkt von AS2 zu AS4 gesendet werden, so kann dies im dargestellten Netzwerk nicht realisiert werden, denn sowohl AS1 als auch AS5 sind als Endnode definiert. Damit wird ein direkter Sitzungsaufbau zwischen AS2 und AS4 verhindert.

LEN = Low Entry Node

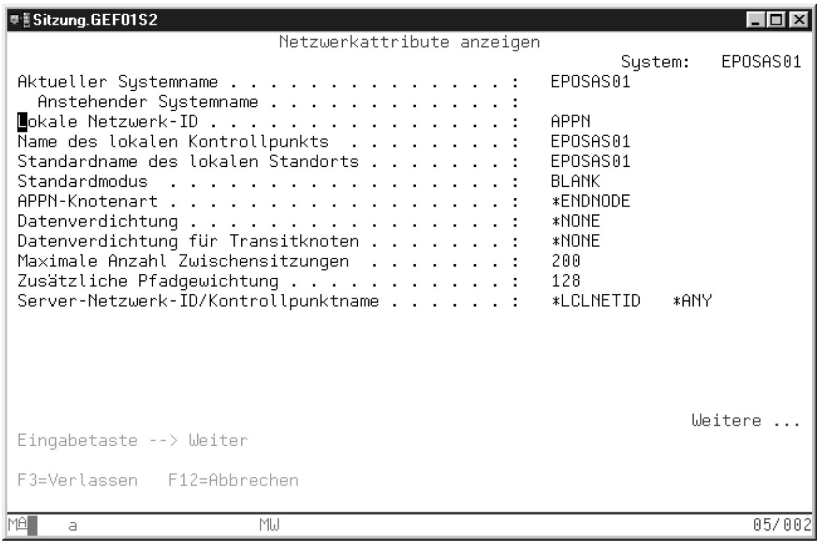
Aber was hat das alles mit unseren PCs zu tun, die wir an die AS/400 anschließen wollen? Auch unsere PCs sind per Definition Bestandteil eines APPN-Netzwerkes – müssen sich also den Adressierungsverfahren eines APPN-fähigen Netzwerks unterordnen.

Ein PC wird in der SNA als Low Entry Node bezeichnet. Mit LEN wird ein System bezeichnet, das einem Endnode oder einem Netnode zugeordnet wird. Ein LEN übernimmt im APPN-

Netzwerk also keine Steuerungsfunktionen, sondern wird durch einen Server an das APPN-Netzwerk quasi angehängt. Damit kann dieser Knotentyp nicht alle Dienste des APPN-Netzwerks steuern und wahrnehmen, er unterliegt lediglich dem Adressierungsverfahren dieses Netzwerktyps.

Was bedeutet das für die Konfiguration von PC-Clients? Das bedeutet, daß der anzubindende PC alle Merkmale eines APPN-fähigen Systems aufweisen muß.

Die für die APPN-Adressierung einer AS/400 notwendigen Werte finden sich in den Netzwerkattributen der AS/400. Geben Sie einfach einmal den Befehl DSPNETA – Netzwerkattribute anzeigen – auf Ihrer AS/400 ein und Sie werden folgenden Bildschirm sehen. Die dargestellten Werte werden sicherlich anders ausfallen, aber das spielt im Moment keine Rolle.



Die Netzwerkattribute der AS/400

Wichtige Adresswerte:

Lokale Netzwerk-ID

Die lokale Netzwerk-ID beschreibt die Zugehörigkeit zu einem logischen Netzwerk. Stellen Sie sich einmal vor Sie haben ein großes, über die ganze BRD verteiltes Netzwerk zu verwalten. Es ist sicherlich für Sie einleuchtend, daß eine Administration einfacher zu organisieren ist, wenn dieser Koloß eines physischen Netzwerks in kleine Untereinheiten gegliedert wird. Diese Untereinheiten werden als logische Netzwerke bezeichnet. Alle die Systeme, die zu einem logischen Netzwerk gehören, besitzen eine identische lokale Netzwerk-ID. Werden also in der Folge PCs in das betreffende logische Netzwerk aufgenommen, so muß diesen PCs ebenfalls eine lokale Netzwerk-ID gegeben werden. Dieses geschieht dann im Rahmen der PC-Konfiguration des IBM Client Access oder anderer Produkte.

Name des lokalen Kontrollpunktes

Der Name des lokalen Kontrollpunktes gibt einem APPN-Knoten einen Namen. Dieser Name muß eindeutig in einem logischen Netzwerk vergeben werden. Der gesamte qualifizierte Name in einem logischen APPN-fähigen Netzwerk setzt sich aus der lokalen Netzwerk-ID und dem Namen des lokalen Kontrollpunktes zusammen. Beide Komponenten werden durch einen Punkt getrennt.

Lokale_Netzwerk-ID.Name_des_lokalen_Kontrollpunktes

Wie Sie aus den Netzwerkattributen meiner AS/400 leicht ersehen können, ist der qualifizierte APPN-Name des Systems:

APPN.EPOSAS01

Auch PCs müssen eine derartig aufgebaute Adresse besitzen, die dann aber mit Hilfe der entsprechenden Client Access-Produkte zu erstellen ist.

Standardname des lokalen Standorts

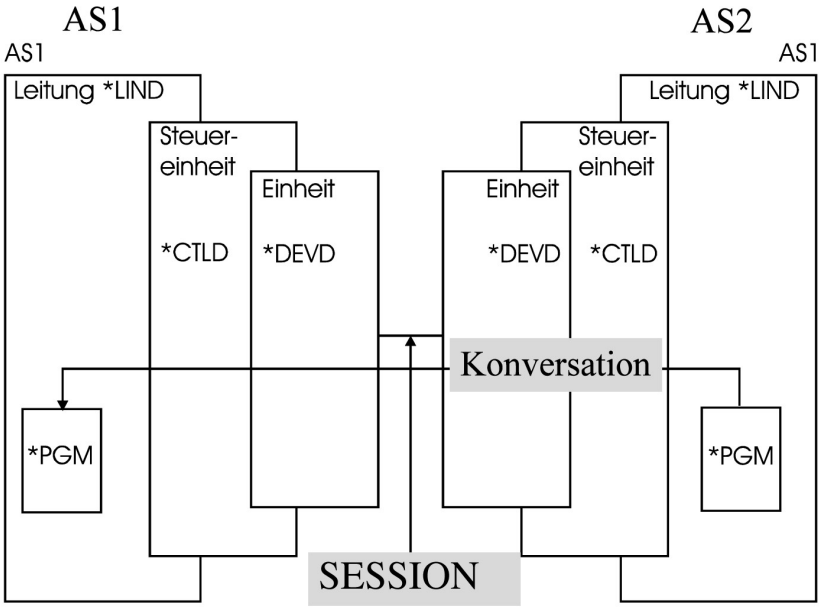
Der Standardname des lokalen Standorts dient zum Sitzungsaufbau zwischen zwei benachbarten SNA-basierten Systemen. D.h., daß mit dieser Adresse ein Zielname für benachbarte Systeme eingerichtet wird. Schließe ich einen PC an meine AS/400 an, so stelle ich die Verbindung her, indem auf dem PC der Standardnamen des lokalen Standorts der AS/400 als Ziel der Verbindung angegeben wird. Bei vielen Konfigurationsprogrammen wird dieser Parameter fälschlich als Systemname bezeichnet.

5.1.1.2 Sitzungen und Konversationen

Eine Sitzung bezeichnet im SNA-Netzwerk das Zustandekommen einer physischen Verbindung zwischen zwei Systemen.

Eine Konversation bezeichnet die Tätigkeit und die Funktionen, die auf Basis der Sitzung realisiert werden.

Welche Objekte werden auf einer AS/400 gebraucht, die dann letztendlich zum Sitzungs- und Konversationsaufbau führen?



Objektverteilung für SNA-Verbindung zwischen zwei AS/400-Systemen

Ich gehe von dem einfachen Bild aus, zwei Systeme AS/400 über eine Ethernet-Leitung lokal miteinander verbinden zu wollen. Das erste System heißt EPOSAS01, das zweite EPOSAS02.

Welche Objekte benötige ich? Ich brauche auf jeder Seite eine funktionierende Leitung, die mittels einer Leitungsbeschreibung konfiguriert und erstellt wird. Weiterhin brauche ich eine Steuereinheit, hierzu erstelle und konfiguriere ich eine Steuereinheitenbeschreibung. Und zu guter Letzt benötige ich eine Einheit, die mit Hilfe einer Einheitenbeschreibung erstellt wird.

Im Folgenden werde ich nicht auf jeden Parameter der Objekte eingehen, sondern mich auf diejenigen beschränken, die zum Aufbau einer Verbindung grundsätzlich notwendig sind.

5.1.1.2.1 Leitungsbeschreibung

Ethernet-Leitungsbeschreibung System EPOSAS01

Mit Hilfe der Leitungsbeschreibung definieren wir die Attribute der physischen Schnittstelle, über die mit dem entfernten System kommuniziert wird

Name der Leitungsbeschreibung

Der Name der Leitungsbeschreibung ist frei wählbar.

Ressourcenname

Der Ressourcenname der Ethernetkarte ist mittels des Befehl WRKHDWRSC *CMN (mit Hardwareressourcen arbeiten) zu ermitteln.

Lokale Adapteradresse

Die lokale Adapteradresse wird direkt aus der Karte ermittelt. Standardwert bei der Eingabe ist *SYSGEN.

Austausch-ID

Die Austausch-ID ist eine achtstellige hexadezimale Adresse, die aus zwei Teilen besteht. Die ersten drei Stellen sind der sogenannte SNA-Block und bezeichnen das jeweils eigene System. Dieser Wert ist nicht frei zu vergeben, folgende Zeichenfolgen sind erlaubt:

056 System AS/400

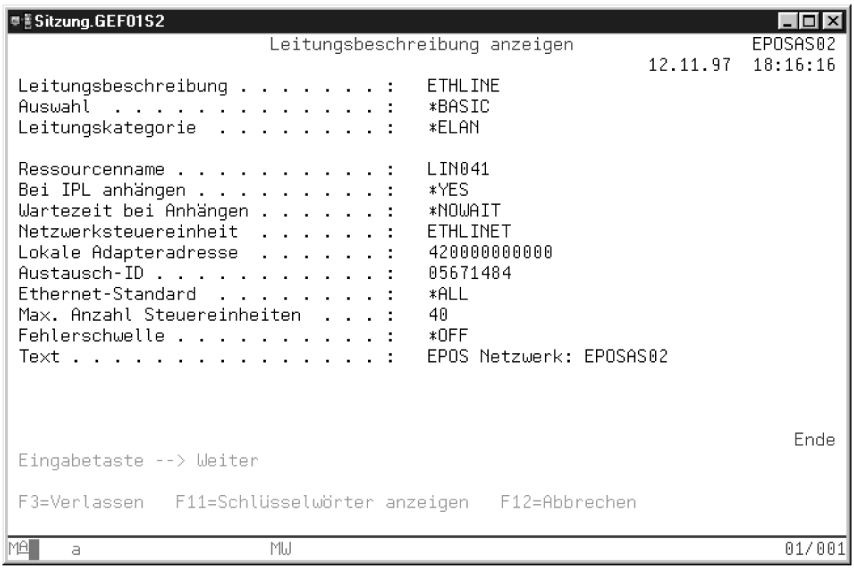
022 System /38

03E System /36

050 PC

Da in unserem Beispiel zwei Systeme AS/400 miteinander verbunden werden sollen, ist der SNA-Block 056 auf beiden Seiten zu wählen.

Wie sieht die Leitungsbeschreibung auf der entfernten Seite aus?



Ethernet-Leitungsbeschreibung System EPOSAS02

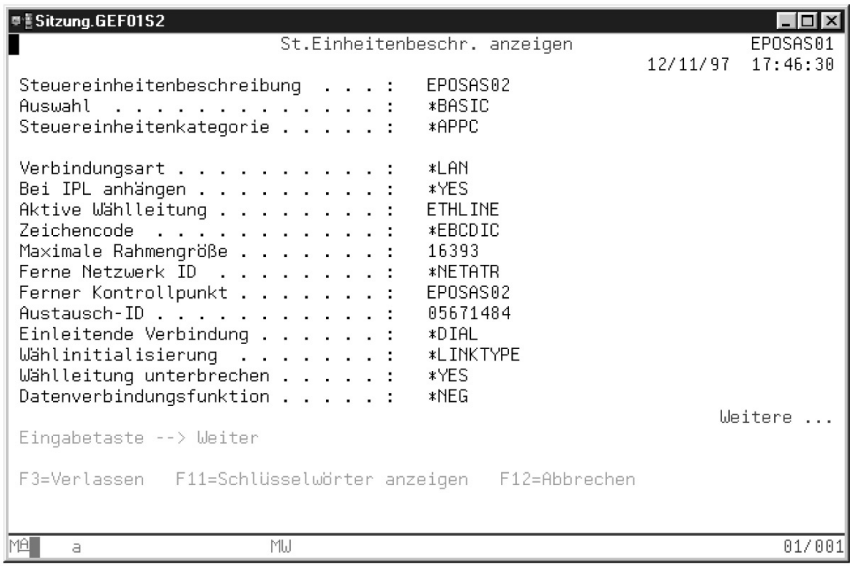
Im Prinzip genauso wie auf der lokalen Seite. In diesem Beispiel sehen wir, daß auf dem System EPOSAS02 ein anderer Ressourcenname verwendet wird.

Die eingebrannte Adresse des Ethernet-Adapters ist mit einer sogenannten virtuellen Adresse überschrieben worden, muß aber im lokalen Netzwerk eindeutig sein.

Bei der Austausch-ID ist ebenfalls der SNA-Block 056 gewählt worden, denn EPOSAS02 ist ein System AS/400.

5.1.1.2.2 Steuereinheitenbeschreibung

Wir befinden uns jetzt wieder auf der EPOSAS01 und sehen uns jetzt die Steuereinheitenbeschreibung auf diesem System an.



Die Steuereinheit für System EPOSAS02 auf EPOSAS01

Der Sinn und Zweck einer Steuereinheit liegt darin, die physikalischen und Adressierungsattribute des Kommunikationspartners zu beschreiben. Ich beschreibe also mit der Steuereinheit auf der EPOSAS01 die SNA-Fähigkeiten der EPOSAS02. Man könnte vereinfachend sagen, die Attribute, die ich in der Leitungsbeschreibung von EPOSAS02 definiert habe, finden sich wieder in der Steuereinheitenbeschreibung von EPOSAS01, und die Leitungsattribute von EPOSAS01 finden sich wieder in der Steuereinheitenbeschreibung von EPOSAS02. Dieses Bild ist

nicht komplett richtig, hilft aber, die Beziehung zwischen diesen Objekten zu verstehen.

Wichtige Parameter (EPOSAS01):

Aktive Wählleitung

Der Name der Leitungsbeschreibung über die die Kommunikation abgewickelt werden soll. In unserem Beispiel heißt die Ethernet-Leitung ETHLINE, also ist dieser Name hier einzutragen.

Ferne Netzwerk-ID

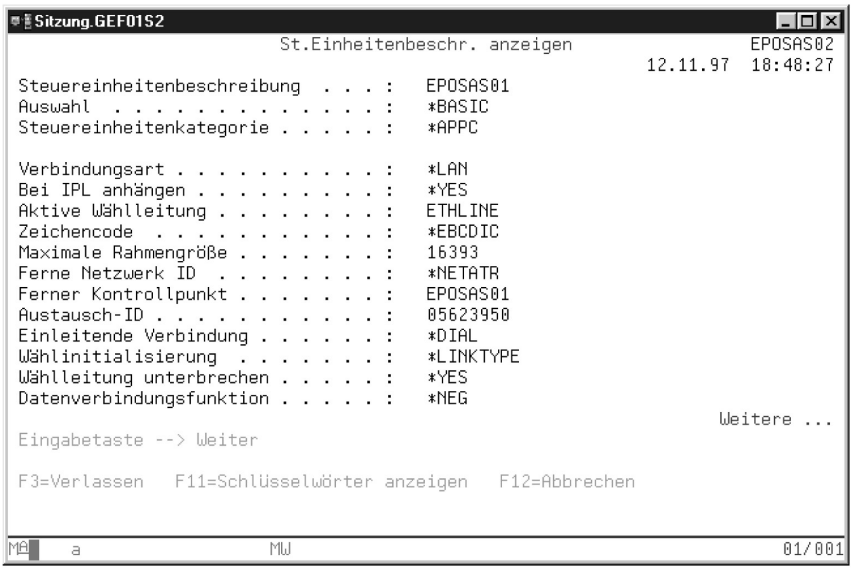
Da das System EPOSAS02 zum gleichen logischen Netzwerk wie das System EPOSAS01 gehört, muß in diesem Parameter auf beiden Seiten die gleiche Netzwerk-ID eingetragen werden. Hier wird mit Hilfe des Einsetzwertes *NETATR auf die lokalen Netzwerkattribute von EPOSAS01 verwiesen. Wichtig ist, daß in den Netzwerkattributen beider Kommunikationspartner die gleiche Netzwerk-ID zu finden ist.

Ferner Kontrollpunkt

In diesen Parameter wird der Name des lokalen Kontrollpunktes der entfernten AS/400 also des Systems EPOSAS02 eingetragen. Damit kennt das System EPOSAS01 den vollständigen APPN-Namen des Kommunikationspartners EPOSAS02: APPN.EPOSAS02

Austausch-ID

Hier finden wir die Austausch-ID aus der Leitungsbeschreibung der EPOSAS02.



Die Steuereinheit für System EPOSAS01 auf EPOSAS02

Wichtige Parameter (EPOSAS02):

Aktive Wählleitung

Der Name der Leitungsbeschreibung über die die Kommunikation abgewickelt werden soll. In unserem Beispiel heißt die Ethernet-Leitung ETHLINE, also ist dieser Name hier einzutragen.

Ferne Netzwerk-ID

Da das System EPOSAS01 zum gleichen logischen Netzwerk, wie das System EPOSAS02 gehört, muß in diesem Parameter auf beiden Seiten die gleiche Netzwerk-ID eingetragen werden. Hier wird mit Hilfe des Einsetzwertes *NETATR auf die lokalen

Netzwerkattribute von EPOSAS02 verwiesen. Wichtig ist, daß in den Netzwerkattributen beider Kommunikationspartner die gleiche Netzwerk-ID zu finden ist.

Ferner Kontrollpunkt

In diesen Parameter wird der Name des lokalen Kontrollpunkt der entfernten AS/400 also des Systems EPOSAS01 eingetragen. Damit kennt das System EPOSAS02 den vollständigen APPN-Namen des Kommunikationspartners EPOSAS01: APPN.EPOSAS01

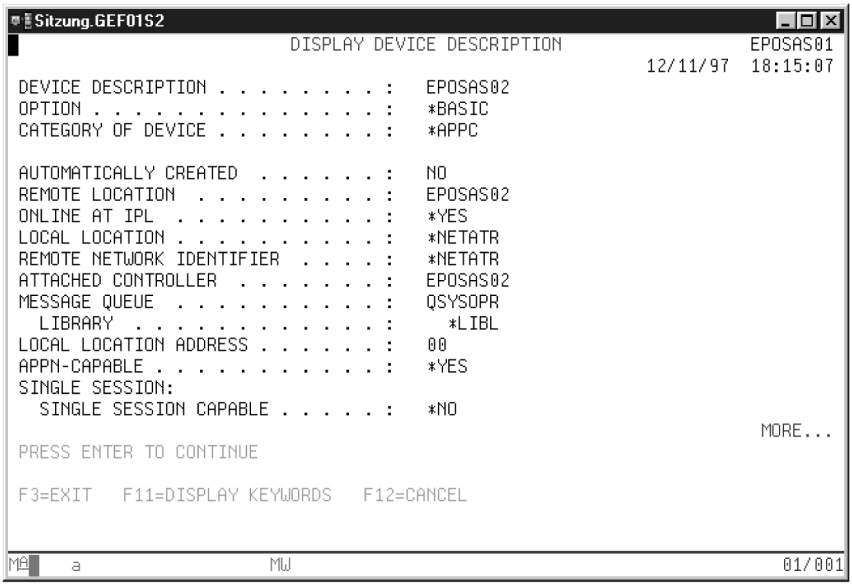
Austausch-ID

Hier finden wir die Austausch-ID aus der Leitungsbeschreibung der EPOSAS01.

5.1.1.2.3 Einheitenbeschreibung

Die Einheitenbeschreibung enthält die Adressdaten zum unmittelbaren Nachbarn.

Sehen wir uns zuerst die Einheitenbeschreibung des Systems EPOSAS01 an.



Die Einheitenbeschreibung für die Adressierung von EPOSAS02 auf der Seite EPOSAS01

Wichtige Parameter (EPOSAS01):

Remote Location – ferner Standort:

Hier tragen wir den Standardnamen des lokalen Standorts von EPOSAS02 ein.

Local Location – lokaler Standort:

Hier kann der Standardname des lokalen Standorts von EPOSAS01 explizit eingetragen werden. Da dieser Name jedoch auf der lokalen Seite (EPOSAS01) in den Netzwerkattributen hinterlegt wurde, referenzieren wir diesen Parameter mit Hilfe des Einsetzwertes *NETATR.

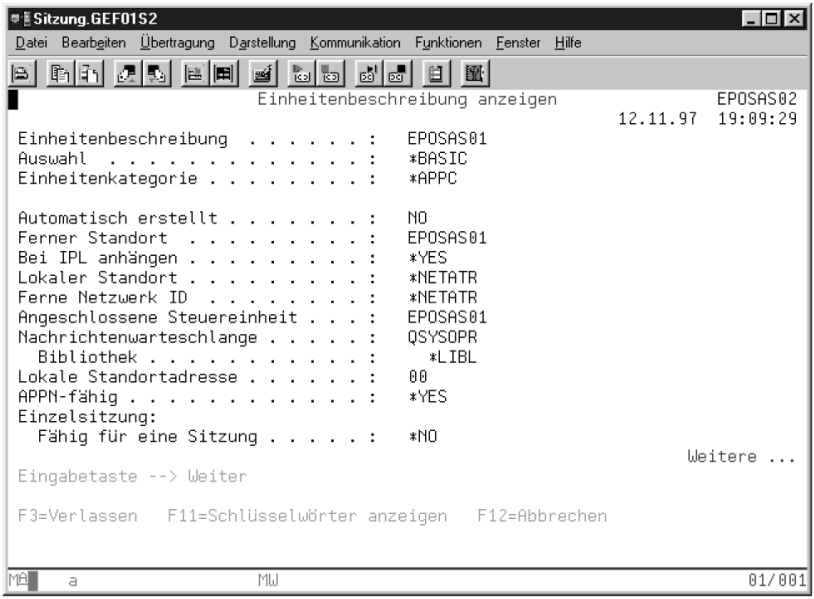
Remote Network Identifier – ferne Netwerk-ID:

Da EPOSAS02 zum gleichen logischen Netzwerk wie EPOSAS01 gehört, bedienen wir uns auch hier der lokalen Netzwerkattribute von EPOSAS01.

Attached Controller – angeschlossene Steuereinheit:

In diesen Parameter tragen wir den Namen der Steuereinheit von EPOSAS01 ein. Somit haben wir die logische Verbindung zwischen der Leitungsbeschreibung, der Steuereinheitenbeschreibung und der Einheitenbeschreibung für das System EPOSAS01 vollständig erstellt.

Sehen wir uns jetzt die Einheitenbeschreibung des Systems EPOSA02 an.



Die Einheitenbeschreibung für die Adressierung von EPOSAS01 auf der Seite EPOSAS02

Wichtige Parameter (EPOSAS02):

Remote Location – ferner Standort:

Hier tragen wir den Standardnamen des lokalen Standorts von EPOSAS01 ein.

Local Location – lokaler Standort:

Hier kann der Standardname des lokalen Standorts von EPOSAS02 explizit eingetragen werden. Da dieser Name jedoch auf der lokalen Seite (EPOSAS02) in den Netzwerkattributen hinterlegt wurde, referenzieren wir diesen Parameter mit Hilfe des Einsetzwertes *NETATR.

Remote Network Identifier – ferne Netwerk-ID:

Da EPOSAS01 zum gleichen logischen Netzwerk wie EPOSAS02 gehört, bedienen wir uns auch hier der lokalen Netzwerkattribute von EPOSAS02.

Attached Controller – angeschlossene Steuereinheit:

In diesen Parameter tragen wir den Namen der Steuereinheit von EPOSAS02 ein. Somit haben wir die logische Verbindung zwischen der Leitungsbeschreibung, der Steuereinheitenbeschreibung und der Einheitenbeschreibung für das System EPOSAS02 vollständig erstellt.

Und was bleibt jetzt noch zu tun? – Die Verbindung muß gestartet werden!

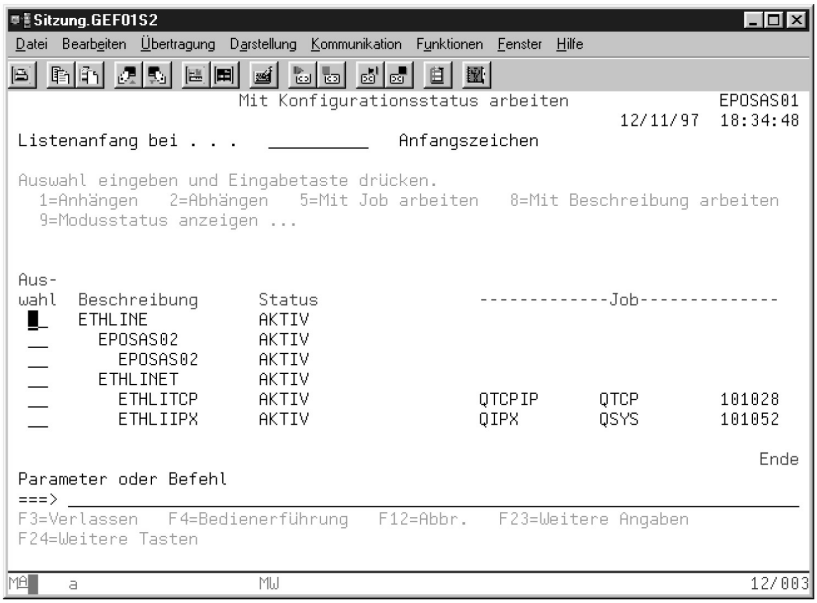
Auf dem System EPOSAS01:

Ich gebe den Befehl WRKCFGSTS *LIN ETHLINE (mit dem Konfigurationsstatus arbeiten) ein und trage dann eine 1=Anhängen im Auswahlfeld vor der Leitungsbeschreibung ETHLINE ein und warte darauf, daß der Leitungsstatus von „Abgehängt“ auf „Anhängen anstehend“ wechselt. Jetzt sollten auch die verbundene Steuereinheit und Einheit sichtbar werden. Auch deren Status sollte auf „Anhängen anstehend“ stehen. Sollte sich dieses Bild nicht ergeben, ist schon eins sicher: Sie haben einen Fehler gemacht!

Auf dem System EPOSAS02:

Sie verhalten sich absolut identisch.

Sollte auch hier alles in Ordnung gegangen sein, so wechselt der Status der Leitung, der Steuereinheit und der Einheit auf aktiv!



WRKCFGSTS *LIN ETHLINE zeigt eine aktive Verbindung für EPOSAS01

Was ist durch das Anhängen der Objekte zwischen den beiden Systemen abgelaufen?

Die Leitung, Steuereinheit und Einheit von EPOSAS01 ist gestartet worden. Davon hat EPOSAS02 nichts bemerkt.

Nachdem aber auf dem System EPOSAS02 ebenfalls diese Objekte aktiviert wurden, hat das System EPOSAS02 seine Austausch-ID an das System EPOSAS01 gesendet. Der Weg zum System EPOSAS01 wurde mit Hilfe des Parameters „Ferner Standort“ aus der Einheitenbeschreibung von EPOSAS02 gefunden – dort steht nämlich „gehe zu EPOSAS01“. Die gesendete Austausch-ID wird jetzt von EPOSAS01 geprüft. Die Prüfung

erfolgt mit Hilfe des Austausch-ID-Parameter in der Steuereinheitenbeschreibung von EPOSAS01, denn hier haben wir ja die Austausch-ID von EPOSAS02 eingetragen. Erkennt EPOSAS01, daß die hier eingetragene Austausch-ID mit der von EPOSAS02 gesendeten Austausch-ID übereinstimmt, so sendet EPOSAS01 seine eigene Austausch-ID an EPOSAS02 und dort findet die gleiche Prüfung statt, nur eben umgekehrt.

Geht die Prüfung von EPOSAS02 ebenfalls erfolgreich aus, so wird eine SNA-Sitzung zwischen den beiden Systemen aufgebaut. Diesen Vorgang erkennen wir äußerlich daran, daß alle Objekte der Verbindung den Status aktiv anzeigen. Werden die Objekte nicht aktiv, so haben wir einen Fehler gemacht. Zur Überprüfung sollte dann in die Nachrichtenwarteschlange von QSYSOPR (Systemoperator) gesehen werden, denn hier wird eine Nachricht aufgelaufen sein, die uns Näheres über den Fehler sagen kann.

Die Sitzung ist aufgebaut heißt, daß beide Systeme ihr Einverständnis erklärt haben, miteinander kommunizieren zu wollen.

So weit, so gut – aber reale kommunikative Tätigkeiten werden nicht ausgeführt. Dazu müssen wir jetzt einen Netzwerkdienst starten. Ich habe einfach einen Arbeitsstationsdurchgriff von EPOSAS01 zum System EPOSAS02 gestartet und sehe mir wieder den Konfigurationstatus meiner Verbindung an (WRKCFGSTS *LIN ETHLINE).

Und jetzt sehen wir den Job EPOSAS01/QUSER/830243. Dieser Job ist Ausdruck dafür, daß zwei Programme – auf der EPOSAS01 und der EPOSAS02 – direkt miteinander kommunizieren, denn der hier sichtbare Job ist durch den Durchgriff von der EPOSAS01 zur EPOSAS02 erzeugt worden. Und dieser Vorgang wird als Konversation bezeichnet.

Sie werden jetzt sicherlich fragen: „Das ist ja alles sehr interessant – aber was hat das mit der Anbindung von PCs zu tun?“ Diese Haltung ist verständlich, denn ein PC kennt keine Leitungsbeschreibungen, Steuereinheitenbeschreibungen und Einheitenbeschreibungen. PCs haben aber „Ersatzkomponenten“, die es Ihnen möglich machen, eine AS/400 zu adressieren und erwarten das Vorhandensein dieser Kommunikationsobjekte.

5.1.2 PCs an ein SNA-Netzwerk anbinden

Für PC-Anbindungen stehen unterschiedliche Produkte zur Verfügung, die eine Anbindung an ein SNA-Netzwerk möglich machen.

Die Konfiguration dieser Komponenten werde ich bei den einzelnen Client Access-Produkten beschreiben. An dieser Stelle gebe ich nur eine kurze Übersicht.

Ich habe die in diese Abteilung gehörenden Connectivity-Produkte in zwei Gruppen eingeteilt:

1. Produkte, die eine Direktadressierung ermöglichen

Hierbei wird eine direkte Datenfernverarbeitungsverbindung zwischen dem jeweiligen PC und der AS/400 aufgebaut.

DOS und Windows 3.1 (1)

IBM LAN Support – ein reiner DOS-Treiber. Kann nicht unter Windows 95 und Windows NT verwendet werden. Wird mit IBM Client Access/400 ausgeliefert.

MSDLC – ein 16-Bit-Treiber der im Windows-Speicher läuft – wird von Microsoft geliefert.

WINDOWS 95

MSDLC-32 – ein 32-Bit-Treiber, der zum Auslieferungsumfang von Windows 95b gehört. Besitzen Sie eine ältere Windows 95-Version, so erhalten Sie einen MDSLC-32-Treiber mit dem Service Pack 1 oder über das Internet.

Windows NT 4.0

DLC Protokoll – das DLC-Protokoll gehört zum Auslieferungsumfang von Windows NT 4.0

2. Gateway-Produkte

Gateways gehen davon aus, daß die PCs im PC-Netzwerk ein PC-basiertes Protokoll verwenden (IPX/SPX: Novell oder NetBeui: Microsoft) und daß ein Gatewaysystem die Verbindungsanforderung zentralisiert über die Protokollumsetzung realisiert und primär die Kommunikation mit der AS/400 abwickelt.

Ich nenne hier die zwei derzeit am Markt wohl am häufigsten eingesetzten Produkte:

Novell

Netware for SAA 2.0 und Netware AS/400-Edition

Microsoft

Microsoft SNA-Server 3.0

5.2 TCP/IP

5.2.1 Einführung

Mit der Freigabe von OS/400 V3 R1 wurde der TCP/IP-Protokollstapel und damit verschiedene TCP/IP-basierte Dienste als integrierter Bestandteil des AS/400-Betriebssystems zur Verfügung gestellt. OS/400 V3 R1 wurde zum Jahreswechsel 1994/1995 freigegeben. Seitdem sind ein paar Jahre ins Land gezogen und wir leben heute mit dem AS/400-Betriebssystem OS/400 V4 R3. Auch dieses Betriebssystem beinhaltete wieder einige neue TCP/IP-Dienste und zeigt erneut, wie stark IBM daran interessiert ist, TCP/IP als „Standardprotokoll" für DVF-Verfahren zu etablieren.

Neben der Funktion, Verbindungen zwischen TCP/IP-fähigen Systemen zu realisieren, gehören zu diesem Protokollstapel eine ganze Reihe von Funktionen und Dienste, von denen viele in OS/400 implementiert sind. Damit Sie mit diesen Begriffen vertraut gemacht werden, stelle ich eine Kurzerläuterung dieser Funktionen an den Anfang dieses Kapitels.

Folgende TCP/IP-Dienste sind bisher implementiert worden:

SNMP – Simple Network Management Protocol

Im TCP/IP-Netzwerk besteht die Möglichkeit der Fernadministration eines Netzwerkes, sofern die beteiligten Hosts das SNMP-Protokoll unterstützen. Soll eine AS/400 als TCP/IP-Host an dieser Fernadministration teilnehmen, muss ein entsprechender SNMP-Server gestartet werden, der dann für die Weiterleitung der Administrationsdaten an den fernen Administrator sorgt.

RouteD – Routing Deamon

Arbeiten Sie mit mehreren TCP/IP-Netzwerken, so können Sie mit Hilfe des RIP-Protokolls Leitwege festlegen, die das beschleunigte Auffinden von anderen TCP/IP-Hosts unterschiedlicher Netzwerke ermöglichen.

BOOTP – Boot Protocol

Das BOOTP-Protokoll ermöglicht den Anschluss von „dummen" NCs und Thin Clients an die AS/400. Dabei sendet der NC seine MAC-Adresse an die verbundene AS/400 , die dann über Einträge in einer sogenannten BOOTP-Tabelle die Verbindung zum NC herstellt und diesem sein Betriebssystem zusendet, sodass er funktionsfähig wird.

DNS – Domain Name Service

Der Domain Name Service ermöglicht es, numerischen TCP/IP-Adressen namensbezogene Adressen zuzuordnen. Diese vergebenen Namen und die ihnen zugeordneten Adressen werden in einer sogenannten Zonendatei gehalten. Ein TCP/IP-Host, der auf einen anderen Host (Zielhost) zugreifen will, geht also zuerst zu dem System, das den Domain Name Service zur Verfügung stellt, und ermittelt mit Hilfe der Zonendatei die numerische Adresse des Zielhost. Bis OS/400 V4 R1 konnte die AS/400 auf einen Domain Name Server zugreifen, ab OS/400 V4 R2 kann die AS/400 einen DNS-Dienst zur Verfügung stellen.

DHCP – Dynamic Host Configuration Protocol

Das DHCP gibt Ihnen die Möglichkeit, TCP/IP Adressen dynamisch im Netzwerk zu verteilen. Sie brauchen also nicht manuell TCP/IP-Adressen zu vergeben, sondern lassen den DHCP-

Server selbständig gültige Adressen vergeben. Die Lebensdauer dieser Adressen hängt dabei von einer vorgegebenen Lease-Zeit (Gültigkeitsdauer der Adresse) ab. So können Adressen nur für den einmaligen Gebrauch generiert werden oder Ihnen kann über eine längere Lease-Zeit eine längere Lebensdauer zugebilligt werden. Es ist durchaus möglich, sich anfänglich durch den DHCP-Server Adressen generieren zu lassen, die dann eine unendliche Lease-Zeit haben, so dass Sie dann mit statischen Adressen arbeiten können.

FTP – File Transfer Protocol

Das File Transfer Protokoll ermöglicht Ihnen die Übertragung von Objekten zu jedem System, das FTP-Dienste realisieren kann. FTP ist auf der AS/400 als Client und als Serverdienst implementiert, so dass Sie Daten von der AS/400 zu einem UNIX-, zu einem Windows NT-System etc. senden bzw. von diesem empfangen können. Ebenfalls können die genannten Systeme Daten zur AS/400 senden und gegebenenfalls empfangen. Zum Aufbau einer FTP-Sitzung ist es notwendig, dass Anwender eine entsprechende Berechtigung für den Zugriff auf den FTP-Server besitzen. Im Falle der AS/400 müssen Sie also als AS/400-Benutzer ein entsprechendes Benutzerprofil besitzen.

Trivial FTP – Triviales File Transfer Protocol

Das triviale FTP ermöglicht ebenfalls die Versendung von Daten, beinhaltet jedoch nicht die Übergabe von Sicherheitsdaten. TFTP ist kein benutzerorientierter Dienst, sondern wird beim Einsatz von NCs benötigt, damit diese zum Start benötigte Dateien und Objekte, nach Erhalt einer TCP/IP-Adresse, herunterladen können.

TELNET – Bildschirmemulation

TELNET stellt eine einfache systemübergreifende Bildschirmemulation zur Verfügung. Benutzen Sie Telnet von AS/400 zu AS/400, so erhalten Sie alle von einer 5250-Bildschirmsitzung übergebenen Attribute. Greifen Sie von einem ASCII-basierten Terminal auf eine AS/400 zu, so werden diverse Attribute des 5250-Bildschirms nicht dargestellt. Eine Sonderform der Telnet-Emulation stellen sogenannte TN3270- und TN5250-Emulationen dar. Diese nutzen das Telnet-Protokoll, übertragen dabei alle Merkmale und Funktionen eines 3270- bzw. 5250-Bildschirms.

LPD/LPR – Line Printer Daemon/Line Printer Requester

Der Line Printer Deamon (LPD) ist ein Druckserver, mit dem Sie direkt aus dem Netzwerk heraus auf einen AS/400 – Drucker aus drucken können. Welcher Drucker der AS/400 Ihnen zur Verfügung steht, hängt von der Berechtigungssituation der AS/400 ab. Der Line Printer Requester (LPR) ist der Client eines LPD. Mit der AS/400 als LPR können die auf die LPDs unterschiedlicher Systemumfelder zugreifen. Ebenso können Sie von einem beliebigen LPR auf den LPD der AS/400 zugreifen. LPR ist dreifach auf der AS/400 implementiert:

1. als Remote Ausgabewarteschlange
   (wird mit dem Befehl CRTOUTQ erstellt),
2. als Netzwerk Druckeinheit
   (Erstellung mit dem Befehl CRTDEVPRT) und
3. als Befehl LPR.

HTTP – HyperText Transport Protocol

Das HTTP-Protokoll ermöglicht es Ihnen, Ihre AS/400 als Internet-Server aufzubauen. Seit OS/400 V4 R1 ist es möglich, mehrere Web-Server auf einer AS/400 zu installieren. Mit Hilfe sogenannter Access-Listen können dann für diese Web-Server eigene Berechtigungssysteme und Umgebungen aufgebaut werden.

Datenstations-Gateway konfigurieren

Das Datenstations-Gateway ermöglicht es Ihnen, AS/400-Bildschirme an einen Internetbrowser zu senden. Dabei werden online 5250-Bildschirme ins HTML-Format konvertiert.

SMTP – Simple Mail Transport Protocol

Das Simple Mail Transport Protocol steuert die Versendung von E-Mails, die dann von einem POP3-Server verwaltet werden können.

POP3 – Post Office Protocol

Der POP3-Server übernimmt die Verwaltung von E-Mails auf der AS/400. Darüber hinaus kann er Adressbuchfunktionen für Clients realisieren und Verbindungen zum Post-Dienst des Office Vision/400 herstellen. Die Verbindung zum POP3-Server der AS/400 wird mittels eines Standard E-Mail-Clients (Microsoft Exchange bzw. Outlook, Netscape Mail etc.) hergestellt.

REXEC – Remote Exec Server

Seit OS/400 V4 R1 ist die AS/400 ein sogenannter Remote Exec Server. Was heißt das? Von jedem TCP/IP-basierten Remote Exec Client können Sie, entsprechende Berechtigungen vorausgesetzt,

Programmprozesse auf der AS/400 starten. Es ist also durchaus möglich, dass ein LINUX-basierter Prozess mit Hilfe eines Remote Exec Client einen Dateitransfer auf der AS/400 startet. Darüber hinaus kann eine AS/400 auch ein Remote Exec Client sein. Dieser Dienst wurde über den CL-Befehl RUNRMTCMD (Fernen Befehl ausführen) auf der AS/400 implementiert. Mit Hilfe des Client Access sind Sie in der Lage, jeden Windows 95/ NT-Rechner zu einem Remote Exec Server zu machen. Mit RUNRMTCMD sind Sie dann in der Lage, von der AS/400 einen PC-Befehl auf dem so konfigurierten Windows-System aufzurufen.

NFS – Netfile Services

Die Net File Services des AS/400 sind ein nicht konfigurierbarer Dienst. Das heißt, dass dieser Dienst immer zur Verfügung steht. Er ist als Verzeichnis QFileSvr.400 im Integrated File System (IFS) der AS/400 implementiert. Indem Sie unterhalb von QFileSvr.400 ein Unterverzeichnis mit dem Hostnamen einer zweiten AS/400 einrichten, erhalten Sie einen Einstieg ins IFS dieser zweiten AS/400. Erfolgreich kann dieser Vorgang aber nur umgesetzt werden, wenn entsprechende Berechtigungen vergeben wurden.

DDM über TCP/IP

Ab OS/400 V4 R2 ist nun auch möglich, DDM-Verbindungen mit Hilfe von TCP/IP zu realisieren. Erste Versuche meinerseits haben gezeigt, dass diese DDM-basierten Dateizugriffe deutlich schneller sind als SNA-basierte.

5.2.2 Verbindungsaufbau

In diesem Kapitel möchte ich mit Ihnen über den Verbindungsaufbau zwischen TCP/IP-fähigen Systemen sprechen. Der Verbindungsaufbau befolgt dabei grundsätzlich unterschiedliche Wege, verglichen mit Systemen, die unter IBM SNA laufen. Um den Verbindungsaufbau beschreiben zu können, werden Sie in der Folge eine Reihe von Begriffen kennen- und verstehen lernen, die grundsätzlich und wichtig für die Funktion und den Betrieb des TCP/IPs sind.

Lassen Sie uns von folgendem einfachen Szenario ausgehen: Wir beabsichtigen, einen PC direkt mit einer AS/400 über ein Ethernet-Netzwerk zu verbinden. Welche Alternativen haben wir?

1. Im Rahmen eines SNA-Netzwerks bauen wir eine DLC-Verbindung auf. Das DLC-Protokoll stellt eine direkte Verbindung zur AS/400 her, d. h. dass beide Systeme eine direkte Verbindung unterhalten. Was wiederum bedeutet, dass beide Systeme eine sogenannte SNA-Sitzung aufbauen müssen. Damit der Sitzungsaufbau erfolgen kann, tauschen beide Systeme sogenannte Austausch-IDs aus. Wird dieser Prozess korrekt abgeschlossen, so werden Benutzerkennungsdaten in der AS/400 überprüft und sollte auch dieser Vorgang korrekt abgeschlossen werden, so wird die Verbindung als entsprechend berechtigt gekennzeichnet. Erst danach kann das eigentliche DFV-Geschäft aufgenommen werden, es können Bildschirmemulationen, Dateitransfers, emulierte und virtuelle Drucker etc. genutzt werden. Diesen Vorgänge werden dann als Konversationen bezeichnet.
   Fazit: Die SNA Sitzung sorgt für die physikalische und logische Verbindung und legt die Sicherheitsdaten der Verbin-

dung fest, die Konversation steuert dann die auf der Basis der Sitzung geforderten Tätigkeiten und Funktionen. So weit so gut, was für Sie wichtig ist: dass es sich bei einer SNA-Verbindung um eine Verbindung zwischen zwei Systemen handelt, denn die Adressen, die wir zu vergeben haben, beziehen sich jeweils auf das gesamte System. Werte, die hierbei zu versorgen sind, sind die Netzwerk-IDs beider Systeme, die lokalen Standortnamen beider Systeme etc. Auf unser kleines Beispiel bezogen führt diese Arbeit dann dazu, dass unser PC nach erfolgreicher Konfiguration unterhalb der Leitungsbeschreibung durch eine APPC-Steuereinheit und durch eine APPC-Device repräsentiert wird – diese beiden Objekte steuern die Sitzung. Alle Tätigkeiten , also die Konversationen, werden dann als Jobs dargestellt.

2. Wir bauen eine TCP/IP Verbindung auf. Der große Unterschied zu der oben beschriebenen Variante besteht darin, dass jetzt keine System-zu-System-Verbindung aufgebaut wird, sondern die Verbindungsaufnahme letztendlich auf der Ressourcen-Ebene vollzogen wird. Was will uns das sagen? Wenn wir eine TCP/IP-Adresse vergeben, wem wird eigentlich eine Adresse gegeben? Die IP-Adresse wird auf der AS/400 als sogenanntes TCP/IP-Interface an die Ethernet-Leitungsbeschreibung gebunden und beim PC wird die Adresse an die Ethernet-Netzwerkkarte gebunden.

   Fazit: die Verbindung erfolgt auf der Ebene der Netzwerkressourcen, also der Netzwerkkarten. Der funktionale Gegensatz zur SNA-Verbindung besteht darin, dass zum Zeitpunkt der Verbindungsaufnahme keine Berechtigungsdaten zwischen den Systemen übertragen werden. Die IP-Adresse beschreibt lediglich, dass ein System in einem TCP/IP-Netzwerk verfügbar ist, dass seine Adresse sozusagen im Netzwerk bekannt

ist und dass dieses System zu einem logischen Netzwerk dazugehört. Mehr nicht! Und wann erfolgt dann die Berechtigungsüberprüfung? Diese erfolgt dann auf der sogenannten Funktionsebene. Immer dann, wenn wir eine TCP/IP-Funktion aufrufen, wird zuerst überprüft, ob ein Benutzer für diese Funktion auch die entsprechenden Rechte besitzt und erst dann wird diese Funktion ausgeführt. Das lässt sich auch sehr leicht nachvollziehen. Gehen Sie einmal an einen PC der mittels TCP/IP auf die AS/400 zugreift und starten Sie einfach eine Bildschirmemulation ohne vorher mit dem Verbindungsmanager die Verbindung aufzubauen. Was passiert? Sie müssen sich zuerst für die Funktion anmelden (nicht für die Verbindung!), erst dann kommt der Bildschirm. Beenden Sie die Emulation und rufen Sie sie dann wieder auf – und was passiert jetzt? Sie müssen sich erst wieder für die Funktion anmelden und danach kommt der Bildschirm.

Die Ursache für dieses komplett unterschiedliche Verhalten beider Verbindungsvarianten liegt sicherlich darin, dass die Anforderungen, die an das TCP/IP-Protokoll gestellt wurden, von denen die an das SNA-Verfahren gestellt wurden, grundsätzlich verschieden sind – Stichwort: offenes Netzwerk. Für uns AS/400-Leute ergibt sich diese Unterschiedlichkeit jedoch aus der Implementation der beiden Schnittstellen. Während das SNA-Verfahren seine Konversationen (siehe oben) auf der Prozessebene des OS/400 abwickelt, also eine Konversation nicht anderes ist, als ein Job des OS/400, den wir in der WRKACTJOB (Mit aktiven Jobs arbeiten) – Anzeige als Verbindungsjob im Subsystem QCMN oder QBASE wahrnehmen, so wird das TCP/IP-Geschäft über eine sogenannte Socket-Schnittstelle im Betriebssystemkern der AS/400 abgewickelt. Oberflächlich betrachtet, finden wir also keinen TCP/IP-Verbindungsjob in den klassischen DFV-Sub-

systemen. Nutzen Sie bereits TCP/IP, so sollten Sie sich einmal mit WRKACTJOB das Subsystem QCMN oder QBASE ansehen und Sie werden sehen, dass Sie nichts sehen – jedenfalls keine Jobs, die TCP/IP-Verbindungen zu den entsprechenden TCP/IP-fähigen Clients darstellen.

Da TCP/IP-Verbindungen auf der Ebene der Funktionen hergestellt werden, muss es für die Menge der TCP/IP-Funktionen eine Schnittstelle geben und diese Schnittstelle wird durch sogenannte TCP/IP-Ports dargestellt. Die Ports kann man sich sehr einfach als Eingänge in die TCP/IP-Schnittstelle vorstellen, wobei jeder Eingang (Port) für eine bestimmte Funktion reserviert ist. Die TCP/IP-Ports werden durchnummeriert von 1 bis 65535, wobei wir jedoch zwei Nummernkreise unterschieden: alle Ports zwischen 1 und 1023 sind sogenannte Standardports, d. h. über Sie werden Standardfunktionen des TCP/IP betrieben. Lesen Sie noch einmal die Einführung zum Kapitel 5.2 TCP/IP, dort habe ich beschrieben welche Funktionen in das TCP/IP der AS/400 implementiert wurden. Jede dieser Funktionen wird durch einen Port repräsentiert. Soll ein bestimmter TCP/IP-Dienst ausgeführt werden, so sendet er zuerst einmal seine Portnummer. Diese wird dann auf der empfangenden Seite gesehen und die Anforderung wird an den entsprechenden TCP/IP-Server weitergeleitet und verarbeitet.

Port	Bezeichnung
5	Remote Job Entry
7	Echo
11	Active Users
13	Daytime
20	File Transfer (Data)
21	File Transfer (Control)
23	Remote Terminal (TELNET)
25	SMTP-Simple Mail Transfer Protocol

Port	Bezeichnung
37	Time
42	Host Name Server
43	Who Is
53	Domain Name Server
67	BOOTP/DHCP Relay Agent Server oder Dynamic Host Configuration Protocol Server
68	BOOTPC/DHCPC Bootstrap Protocol Client oder Dynamic Host Configuration Protocol Client
69	Trivial File Transfer Protocol
70	Gopher
79	Finger
80	World Wide Web HTTP
101	Host Name Server
102	ISO TSAP
103	X.400
104	X.400 SND
105	CSNET Mailbox Name Server
109	Post Office Protocol (POP2)
110	Post Office Protocol (POP3)
111	RPC Portmap
137	NetBIOS Name Service
138	NetBIOS Datagram Service
139	NetBIOS Session Service
161	Simple Network Management Protocol (SNMP)
247	Subnet Broadcast Trivial File Transfer Protocol
512	Remote command execution (REXEC)
515	Remote printing (LPD)

Alle Ports im Nummernkreis 1 bis 1023 werden als sogenannte Standard Ports bezeichnet. Standard steht für den Sachverhalt, dass ausschließlich Standard-TCP/IP-Dienste, die in allen Implementationen vorhanden sind, diese Ports benutzen. Ports mit einer Portnummer ab 1024 sind dann sogenannte Individual-ports oder auch kurzlebige Ports. Ein gutes Beispiel für einen Individialport stellt die Funktion des IBM HTTP Workstation-gateways dar. Diese verwendet nämlich den Port 5061. Damit ist eigentlich klar, dass das Workstation-Gateway keine Standardfunktion des TCP/IPs ist, sondern eine Individual-funktion, die wir nicht unbedingt in anderen TCP/IP-Implementationen erwarten können.

Damit aber diese Funktionen für die Jobebene des OS/400 verfügbar werden, müssen diese Ports (Funktionen) auf der Jobebene gesteuert und überwacht werden. Dazu dienen die sogenannten TCP/IP- Server. Bei jedem Start der AS/400 müssen diese Port-Überwachungsserver gestartet werden. Damit es einen Sinn macht, diese Server zu starten, müssen folgende Voraussetzungen gegeben sein:

– Der Netzwerkschnittstelle muss ein TCP/IP-Interface hinzugefügt worden sein. Auf gut deutsch: Erfassen Sie für die Netzwerkschnittstelle der AS/400 eine IP-Adresse (ADDTCPIFC – TCP/IP Interface hinzufügen).

– Die Schnittstelle muss gestartet werden (STRTCPIFC – TCP/IP Interface starten).

Jetzt können die TCP/IP-Server gestartet werden mit dem Befehl STRTCPSVR (TCP/IP-Server starten). Dieser Befehl kennt nur einen Parameter, der den Namen SERVER trägt. Folgende Parameterwerte sind möglich:

Wert	Bezeichnung
*ALL	Alle TCP/IP-Server starten, für die das Attribut AUTOSTART auf *YES gesetzt wurde
*SNMP	Start des SNMP-Agenten
*ROUTED	Start des Router Demons
*BOOTP	Start des Bootp-Servers
*TFTP	Start von Trivial FTP
*DNS	Start des Domain Name Service
*DHCP	Start des DHCP-Servers
*DDM	Start des DDM over TCP/IP
*TELNET	Start des Telnet Servers
*FTP	Start des FTP-Servers
*SMTP	Start des SMTP-Servers
*LPD	Start des TCP/IP Druckservers
*HTTP	Start des Webservers
*WSG	Start des Workstation Gateways
*POP	Start des POP3 – Servers
*REXEC	Start des Remote Exec Servers

Einige dieser Server werden automatisch gestartet: *TELNET, *FTP, *LPD, *HTTP und *POP. Nehmen wir einmal an, Sie beabsichtigen das Workstation-Gateway separat zu starten, so geben Sie einfach den Befehl STRTTCPSVR *WSG ein und dann wird dieser Server gestartet.

Sie können sich aber grundsätzlich die Arbeit einfacher machen, indem Sie den Befehl STRTCP (TCP/IP starten) ohne jegliche Parameter aufrufen. Was passiert jetzt? Dieser Befehl erwartet zwei Parameter:

1 STRSVR – zu startende Server

2. STRIFC – zu startende Schnittstellen

Beide diese Parameter sind mit dem Wert *YES vorbelegt, so dass alle TCP/IP-Server deren AUTOSTART-Parameter auf *YES gesetzt wurden, automatisch gestartet werden. Der zweite Parameter sorgt dafür, dass alle definierten und funktionsfähigen Schnittstellen gestartet werden.

Es ist sicherlich für Sie eine einfache Routine, den Befehl STRTCP in das Autostartprogramm der AS/400 aufzunehmen, so dass alle TCP/IP-Interfaces mit jedem Start des System aktiviert werden.

Nachdem wir uns mit Hintergrundwissen beschäftigt haben – was meiner Meinung nach wichtig ist, um das TCP/IP vernünftig nutzen zu können – wenden wir uns im nächsten Abschnitt den eher handfesten Dingen zu. Als da wären: Erstellung eines TCP/IP-Interface auf der AS/400, TCP/IP für einen Windows-PC aktivieren.

5.2.3 Adressierung

Nachdem wir im vorherigen Abschnitt über den Verbindungsaufbau in einem TCP/IP-Netzwerk, Ports und Serverprogramme gesprochen haben, kümmern wir uns jetzt darum, wie eine IP-Adresse aufgebaut ist und wie eine AS/400 unter TCP/IP adressierungsfähig gemacht wird. Das Umfeld in dem wir uns dabei gedanklich bewegen ist das eines lokalen Ethernet-Netzwerks.

Die IP-Adresse besteht aus einer zweiunddreißig Bit langen Folge von 0 und 1. Jeweils ein Byte also acht Bit werden durch eine Dezimalzahl repräsentiert. Somit ergibt sich, dass eine IP-Adresse aus vier ein Byte langen Dezimalwerten zusammengesetzt ist, diese Werten werden dann jeweils durch einen Punkt getrennt.

Formal betrachtet sieht eine IP-Adresse folgendermaßen aus:

n.n.n.n

Wobei n für einen Wert zwischen 0 und 255 steht. Null repräsentiert die Bitfolge 00000000 und 255 repräsentiert die Bitfolge 11111111.

Hieraus ergibt sich, dass die IP-Adresse 172.16.0.1 eine zumindest formal betrachtet richtige IP-Adresse ist. Um aber bewerten zu können, ob diese Adresse auch funktional korrekt ist, müssen wir die Struktur einer IP-Adresse genauer kennen.

Jede IP-Adresse teilt sich grundsätzlich in zwei Einheiten auf – in die sogenannte Net-ID und die Host-ID. Die Net-ID beschreibt dabei die Zugehörigkeit zu einem logischen Netzwerk, während der zweite Teil, die Host-ID, die Adresse der Arbeitsstation darstellt.

Net-IDs zu vergeben, liegt der Gedanke zugrunde, dass ein physisches Netzwerk als Einheit betrachtet unter Umständen verwaltungstechnisch zu inflexibel ist. Deshalb erscheint es sinnvoll, die physische Einheit eines Netzwerks in logische Untereinheiten zu zergliedern, so dass kleinere organisatorisch einfachere Einheiten entstehen, die besser administriert werden können und bei denen sich der Netzwerkverkehr besser formal beschreiben läßt und deren Schnittstellen besser kontrolliert werden können.

Insofern unterscheidet sich ein TCP/IP-basiertes Netzwerk nicht grundsätzlich von einem SNA Netzwerk. Auch hier kennen wir die lokale Netzwerk-ID als Beschreibungselement für die Zugehörigkeit zu einem logischen Netzwerk.

Die Host-ID gibt dann einem TCP/IP- Host im logischen Netzwerk eine eindeutige Adresse. Der Begriff des Host sollte aber nicht missverstanden werden. Ein TCP/IP-Host entspricht im SNA-Netzwerk einem Knoten. Host beschreibt also nicht die Steuerungsfunktion eines Systems im Netzwerkbetrieb, sondern beschreibt lediglich ein EDV-System im TCP/IP Netzwerk. So ist eine TCP/IP-fähige AS/400, ein UNIX-System, ein PC unter Windows NT, ein Windows 95-Notebook, also jedwedes TCP/IP-fähige System ein Host im TCP/IP-Netzwerk.

Insgesamt gesehen ist also die Struktur einer IP-Adresse zumindest nicht unähnlich einer SNA-Knotenadresse. Der Unterschied besteht jedoch darin, dass die Grenze zwischen der Net-ID und der Host-ID variabel gehalten ist.

Strukturell betrachtet kann eine IP-Adresse folgende Erscheinungsformen haben.

N.H.H.H

N.N.H.H

N.N.N.H

N steht für Net-ID. und H steht für Host-ID.

Alle eben beschriebenen Adressstrukturen sind nicht nur möglich, sondern auch richtig! Die Frage, die sich daraus ergibt, ist: Welcher steuernde Parameter bewirkt die Struktur einer Adresse? Das Geheimnis liegt darin, dass IP-Adressen in sogenannte Adressklassen unterschieden werden.

Derzeit werden im Internet drei Adressklassen verwendet – Class A-, Class B- und Class C-Adressen. Über welches Unterscheidungsmerkmal bilden sich diese Adressklassen heraus? Zur Unterscheidung wird das erste Byte einer IP-Adresse herangezogen.

Class A

Adressenbereich: 1.0.0.1 – 126.255.255.254

Class B

Adressenbereich: 128.0.0.1 – 191.255.255.254

Class C

Adressenbereich: 192.0.0.1 – 223.255.255.254

Steht im ersten Byte einer IP-Adresse ein Wert zwischen 0 und 126, so ist dieses eine Class A-Adresse. Der Inhalt der anderen Stellen kann dann theoretisch jeweils in den Grenzen von 0 bis 255 liegen. Damit hat die vergebene Adresse dann die Struktur N.H.H.H. Also wäre eine IP-Adresse 57.89.0.1 plausibel. Der Wert 57 stellt die Net-ID dar, während die Werte 89.0.1 die Host-ID beschreiben. Alle Hosts, die die Net-ID 57 haben, sind damit Bestandteil des gleichen logischen Netzwerks.

Steht im ersten Byte einer IP-Adresse ein Wert zwischen 128 und 191, so liegt eine Class B-Adresse vor. Auch hier gilt, dass der Inhalt der restlichen Stellen wiederum zwischen 0 und 255 liegen kann. Eine Class B-Adresse hat die Struktur N.N.H.H. Damit wäre die am Anfang dieses Abschnitts abgebildete Adresse 172.16.0.1

nicht nur formal richtig. Das Wertepaar 172.16 ist in diesem Fall als Net-ID zu betrachten, hingegen ist das Wertepaar 0.1 die Host-ID. Daraus ergibt sich, dass all die Systeme, die die Net-ID 172.16. haben, zum gleichen logischen Netzwerk gehören.

Steht im ersten Byte einer IP-Adresse ein Wert zwischen 192 und 223, so handelt es sich um eine Class C-Adresse. Alle anderen Stellen liegen auch hier in den Grenzen zwischen 0 und 255. Eine Class C-Adresse hat die Struktur N.N.N.H. Die IP-Adresse 195.10.99.10 ist damit eine gültige Class C-Adresse. Die ersten drei Stellen 195.10.99 werden jetzt bei Netzwerkvorgängen als Net-ID verstanden, die letzte Stelle, 10, ist die Host-ID. Alle Hosts, die die Net-ID 195.10.99 aufweisen, gehören damit zum selben logischen Netzwerk.

Soweit, so gut – aber wozu ist das nützlich? In der Klassifizierung von IP-Adressen beschreiben wir letztendlich die Dimensionen unseres Netzwerks. Ein Class A-Netzwerk mit seiner einstelligen Net-ID kann theoretisch in 126 logische Netzwerke unterteilt werden, jedes einzelne logische Netzwerk kann jedoch eine großen Menge an Hosts umfassen. Ein Class B-Netzwerk kann dagegen in eine noch größere Anzahl an logischen Netzwerken unterteilt werden, wobei dann aber jedes dieser Netzwerke weniger Hosts adressieren kann. Ein Class C-Netzwerk kann noch feinfühliger in logische Netzwerke zerteilt werden, aber jedes dieser Netzwerke kann nur maximal 255 Hosts haben.

Ich habe ganz bewußt darauf verzichtet, Ihnen die numerischen Grenzwerte zu nennen, denn schon ein Class A-Netzwerk dürfte, zumindest für ein lokales Netzwerk, genügend logische Gliederungsmöglichkeiten bieten.

5.2.3.1 Die privaten Adressen

Sie müssen immer bedenken, dass es sich bei TCP/IP-Adressierungsverfahren um ein weltweit angewendetes Verfahren handelt. Um jetzt Namensdubletten mit dem Internet zu vermeiden, gibt es in jeder Adressklasse einen sogenannten privaten oder freigelassenen Bereich.

Freie Class A Adressen:	10.0.0.0 – 10.255.255.255
Freie Class B Adressen:	172.16.0.0 – 172.31.255.255
Freie Class C-Adressen:	192.168.0.0 – 192.168.255.255

Arbeiten wir in einem LAN (Local Area Network), also einem privaten, nichtöffentlichen Netzwerk, so sollten wir uns immer im Bereich privater Adressen aufhalten. Damit sind wir zuerst einmal davor sicher, eine Adresse zu verwenden, die schon einmal im Internet vergeben wurde. Auf der anderen Seite ist kein Internet-Provider in der Lage, eine Information direkt an eine private Adresse durchzurouten, so dass eine private Adresse auch als eine Art Schutzmechanismus verstanden werden kann.

5.2.3.2 Subnetzmasken

Mit Hilfe der Adressklassen dimensionieren wir unsere Netzwerke nach außen hin. Um aber auch intern zu einer differenzierten Struktur zu kommen, muss jeder IP-Adresse eine sogenannte Subnetzmaske zugeordnet werden.

Subnetzmasken zu definieren, ist eigentlich recht einfach. Jedoch differenziert deren Funktionalität zu verstehen, ist eine nicht so

einfache Aufgabe! Aber nur wer die Funktion der Subnetzmasken richtig versteht, ist in der Lage, ein TCP/IP Netzwerk richtig zu strukturieren und deshalb werde ich mit Ihnen in der Folge deren Art und Funktion ergründen.

5.2.3.2.1 Standard-Subnetzmasken

Die Teilnetzmaske oder auch Subnetzmaske einer IP-Adresse muss mit einem eindeutigen Wert versorgt werden. Die Online-Hilfen der meisten TCP/IP-Implementationen führen dann die folgenden Werte auf, deren Eintragung von der Adressklasse einer avisierten IP-Adresse abhängt.

Class A Adresse:	255.0.0.0
Class B Adresse:	255.255.0.0
Class C-Adresse:	255.255.255.0

Verfahren Sie derartig, so wird Ihre TCP/IP-Schnittstelle funktionieren. Das ist gut, aber Sie sollten sich jetzt die Frage stellen, was Sie mit diesen Werten an- oder ausgerichtet haben und welche Funktionalität sich dahinter verbirgt.

5.2.3.2.2 Struktur der Subnetzmaske

Die Subnetzmaske ist eine 32-Bit lange Folge von binären Einsern und Nullen. Aufgrund der besseren Lesbarkeit hat man diese Binärfolge in vier sogenannte Oktets unterteilt, wobei jedes dieser Oktets Werte in den Grenzen von 00000000 bis 111111111 enthalten kann. Diese Binärwerte werden dann durch Dezimalwerte in den Grenzen von 0 bis 255 (zumindest rein theoretisch)

repräsentiert. Kommt Ihnen das bekannt vor? Eine IP-Adresse ist vom Aufbau her identisch – aber nicht von der Funktion! Um es klarzustellen: Eine Subnetzmaske ist keine Adresse.

Aber was ist sie dann?

5.2.3.2.3 Funktion der Subnetzmaske

Eine Subnetzmaske ist eine Schablone, die als Binärfolge über die Binärfolge der IP-Adresse gelegt wird und definiert, welcher Teil der IP-Adresse als Net-ID ausgewertet wird und welcher Teil der IP-Adresse als Host-ID betrachtet wird. Aber Halt! Es wird doch auch durch die Adressklasse definiert, wie eine IP-Adresse strukturiert ist. Stimmt, aber durch die Historie des TCP/IPs hat es sich so entwickelt, dass wir zwei Verfahren haben, die bestimmen, wie eine IP-Adresse hinsichtlich der Verteilung von Net-ID und Host-ID interpretiert wird. Beide Verfahren sind notwendig und bauen aufeinander auf. Ich kann also nicht sagen: „Ich arbeite nur mit Adressklassen, Subnetzmasken interessieren mich nicht."

Da wir jetzt wissen, was eine Subnetzmaske macht, stellt sich als nächstes die Frage, wie sie ihre Arbeit ausführt. Das wollen wir uns an einem Beispiel verdeutlichen. Gehen wir einfach einmal davon aus, dass ich für die Ethernetkarte meiner AS/400 die Class B IP-Adresse 172.16.0.1. vergebe. Diese Adresse müssen wir uns jetzt als Binärfolge vorstellen:

IP-Adresse (dezimal)	172	16	0	1
IP-Adresse (binär)	10101100	00010000	00000000	00000001

Da wir jetzt für unsere IP-Adresse eine Subnetzmaske zu vergeben haben, werden wir uns zuerst einmal Adressklassen-konform verhalten. Die in der Tabelle dargestellte IP-Adresse gehört der Adressklasse B an. Um eine für die Adressklasse konforme Subnetzmaske zu vergeben, muss ich wie folgt vorgehen:

IP-Adresse (dezimal)	172	16	0	1
IP-Adresse (binär)	10101100	00010000	00000000	00000001
Subnetz-maske (dezimal)	255	255	0	0
Subnetz-maske (binär)	11111111	11111111	00000000	00000000

Um den Vorgang besser verdeutlichen zu können, sollten Sie jetzt nur die Binärfolgen der IP-Adresse und der Subnetzmaske betrachten:

IP-Adresse (binär)	10101100	00010000	00000000	00000001
Subnetz-maske (binär)	11111111	11111111	00000000	00000000

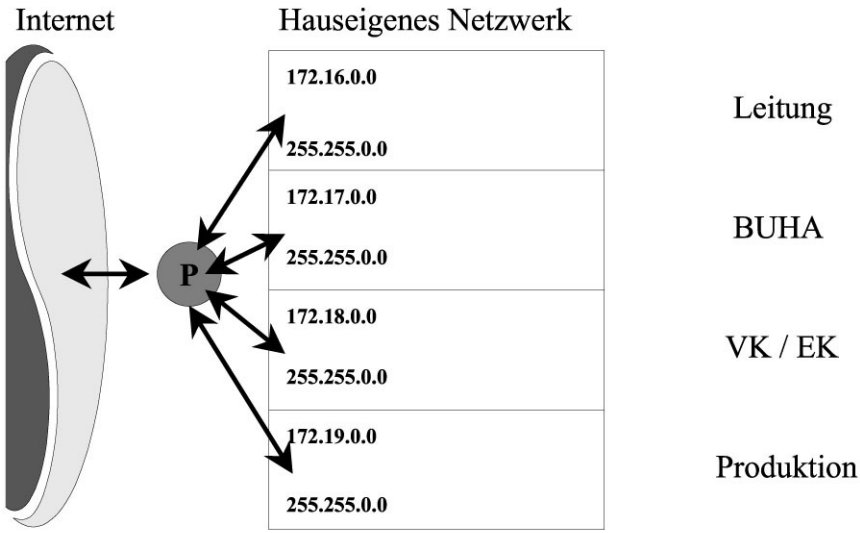
Ich hatte gesagt, dass die Subnetzmaske eine Schablone ist, die über die IP-Adresse gelegt wird. Folgendes wird jetzt realisiert: Steht ein Bit der Subnetzmaske auf 1, so wird das „darunterliegende“ Bit der IP-Adresse als Net-ID interpretiert. Was bedeutet das für unser Beispiel? Jedes Bit des ersten Bytes der IP-Adresse und jedes Bit des zweiten Bytes der IP-Adresse wird als Net-ID ausgewertet. Das ist doch die gleiche Aussage, die mittels der Adressklasse B ebenfalls formuliert wird! Richtig! Wir wollten ja auch eine der Adressklasse B konforme Subnetzmaske vergeben.

Bitte beachten Sie: Eine Subnetzmaske muss immer mit einer geschlossenen Folge von binären Einsen beginnen. Steht ein Bit der Subnetzmaske auf Null, so müssen alle folgenden Bits ebenfalls binär Null sein.

Sie werden sich jetzt sicherlich sagen: „Na gut, wenn es denn so ist, dass es zwei Verfahren gibt, die ich benutzen muss, dann mache ich mir das Leben einfach und verwende nur Adressklassen-konforme Subnetzmasken.“ In kleinen, relativ übersichtlichen TCP/IP-Netzwerken dürften Sie auch mit dieser Haltung zum Erfolg kommen. Werden die Netzwerke größer und komplexer, so wird dieser Ansatz nicht mehr funktionieren.

5.2.3.2.4 1. Beispiel-Netzwerk

Nehmen wir einmal an Sie haben folgendes Netzwerk aufzubauen:



Das hauseigene Netzwerk

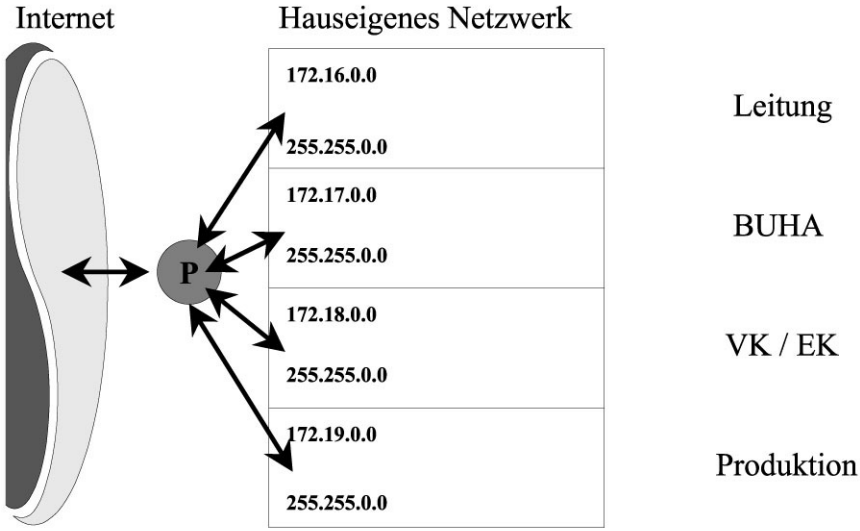
Aufgabe war es, ein TCP/IP Netzwerk einzurichten. Jede Abteilung sollte aber einen eigenen Bereich besitzen, so dass nicht alle Clients aller Abteilungen überall adressierungsfähig sein sollten. Wir sehen das hauseigene Netzwerk dargestellt durch den viergeteilten Kasten in der Mitte des Bildes. Jede Ebene in diesem Kasten beschreibt eine Abteilung. Der Netzwerkdesigner hat jetzt unter der Prämisse gearbeitet, dass ausschließlich adressklassenkonforme Subnetzmasken vergeben werden und hat deshalb für jede Abteilung ein eigenes logisches Netzwerk aufgebaut. Die Geschäftsleitung hat das Netzwerk 172.16.0.0, die Buchhaltung

das Netzwerk 172.17.0.0, der Verkauf/Einkauf das Netzwerk 172.18.0.0 und die Produktion das Netzwerk 172.19.0.0. Soll nun die Geschäftsleitung in Bereiche der Buchhaltung sehen, so sind entsprechend den Anforderungen sogenannte Router aufzubauen. Router sind im TCP/IP-Netzwerk Hosts in einem logischen TCP/IP-Netzwerk, die die Adressen von Hosts in einem zweiten logischen TCP/IP-Netzwerk kennen. Über Router werden wir uns später noch unterhalten. Damit ist der Übergang zwischen den logischen Netzwerken geregelt. Soweit könnte nun alles gut sein und ich bin überzeugt, dass das Netzwerk auch gut funktionieren wird.

Jetzt wird an den Netzwerkadministrator eine weitere Anforderung herangetragen: „Wir müssen ins Internet“. Da nicht jeder, der ins Internet will, so ohne weiteres dort auch hineinkommt, sondern einen Provider (P) braucht, wird dieser kontaktiert. Der Provider analysiert das Netzwerk und stellt fest, dass Sie insgesamt vier Netzwerke haben – das Netzwerk 172.16.0.0, 172.17.0.0, 172.18.0.0 und 172.19.0.0. Sollen also Teilnehmer aus allen vier Netzwerken ins Internet, brauchen Sie vier Internetzugänge (TCP/IP-Profis werden jetzt sicherlich sagen, dass man an dieser Stelle diese Problematik abfangen könnte, so haben sie recht. Ich möchte nur aus Gründen der Einprägsamkeit das Umfeld wie dargestellt sehen). Sicherlich freut sich der Provider, dass er vier Internetzugänge verkaufen kann, den Netzwerkadministrator und seine Firma freut es mit Sicherheit nicht.

5.2.3.2.5 Ein weiteres Beispiel-Netzwerk

Wie können wir diese Problematik unterlaufen. Indem wir uns den Subnetzmasken anvertrauen und unser Netzwerk modifizieren. Die von uns eingesetzte Subnetzmaskentechnik wird erreichen, dass wir nach Außen hin, also zum Internet, als ein Netzwerk erscheinen, aber nach innen als vier Netzwerke.



Sie sehen im Bild, was der Netzwerkadministrator geändert hat. Statt mit vier logischen Netzwerken zu arbeiten, wird im gesamten hauseigenen Netzwerk mit einem logischen Netzwerk gearbeitet (Alle Abteilungen sind Bestandteil des Netzwerks 172.16.0.0.). Damit im hauseigenen Netzwerk jedoch vier sogenannte Subnetze existieren, hat der Administrator die Werte für die Subnetzmasken geändert.

IP-Adresse (dezimal)	172	16	0	1
IP-Adresse (binär)	10101100	00010000	00000000	00000001
1. Subnetz (dez.)	255	255	128	0
1. Subnetz (bin.)	11111111	11111111	10000000	00000000
2. Subnetz (dez.)	255	255	192	0
2. Subnetz (bin.)	11111111	11111111	11000000	00000000
3. Subnetz (dez.)	255	255	224	0
3. Subnetz (bin.)	11111111	11111111	11100000	00000000
4. Subnetz (dez.)	255	255	224	0
4. Subnetz (bin.)	11111111	11111111	11110000	00000000

Konzentrieren wir uns jetzt noch einmal auf die Binärfolgen der Subnetzmasken:

IP-Adresse (binär)	10101100	00010000	00000000	00000001
1. Subnetz (bin)	11111111	11111111	10000000	00000000
2. Subnetz (bin)	11111111	11111111	11000000	00000000
3. Subnetz (bin)	11111111	11111111	11100000	00000000
4. Subnetz (bin)	11111111	11111111	11110000	00000000

Jetzt sehen wir, was passiert ist. Im 1. Subnetz (Leitung) werden nicht nur die ersten beiden Bytes als Net-ID aufgelöst, sondern zusätzlich wird auch noch das erste Bit des dritten Bytes der IP-Adresse als Net-ID ausgewertet. Im zweiten Subnetz wird das nächste Bit, im dritten Subnetz ein weiteres Bit und im vierten Subnetz das vierte Bit mit zur Net-ID hinzugenommen.

Den Übergang zwischen den einzelnen Abteilungssubnetzen wird dann wieder durch entsprechende Router geregelt.

Soweit, so gut. Wo liegt die Einschränkung dieser Lösung? Gehen wir einfach einmal von der Tatsache aus, dass das Netzwerk erweitert werden muss. Weitere Abteilungen oder Teile bestimmter Abteilungen sollen wieder jeweils isolierte Netzwerkbereiche bekommen. So ergibt sich, dass ich maximal nur acht (8) Subnetze mit Hilfe dieses Lösungsansatzes realisieren kann. Wieso? Ganz

einfach: da ja für die Subnetzmasken die Regel besteht, dass eine Subnetzmaske mit einer geschlossenen Folge von binären Einsen beginnen muss und dann an einem definierten Punkt auf eine geschlossenen Folge von binären Nullen „umkippen“ muss, so ergibt sich, dass wir bei diesem Lösungsweg lediglich das dritte Byte der IP-Adresse als Netz-ID mit auswerten dürfen. Das heisst, dann folgerichtig, dass im dritten Byte meiner IP-Adresse nur folgende Werte möglich sind:

3. Byte der Subnetzmaske (binär)	3. Byte der Subnetzmaske (dezimal)
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

Wenn ich mir diesen Sachverhalt vor Augen halte, muss ich auch eingestehen, dass ich nicht mehr als acht (8) Subnetze bilden kann. Und das kann sicherlich nicht der Weisheit letzter Schluss sein – oder?

5.2.3.2.6 Ein drittes Beispiel-Netzwerk

Die Voraussetzung für dieses Netzwerk sind identisch mit denen der bereits besprochenen. Ich möchte nur jetzt eine Netzwerkstruktur erzeugen, die eine flexiblere Lösung anbietet. Ich vergebe also folgende IP-Adressen und Subnetzmasken:

Abteilung	IP-Adresse	Subnetzmaske
Leitung	172.16.0.0	255.255.224
BUHA	172.16.0.0	255.255.224
VK/EK	172.16.0.0	255.255.224
Produktion	172.16.0.0	255.255.224

Was ist das? Ich arbeite lediglich mit einer Subnetzmaske. Aber sind meine Adressen dann nicht Mitglieder ein und desselben Netzwerks? Das hängt jetzt von der Vergabe der Host-ID in den IP-Adressen ab. Lassen Sie uns das einmal genauer betrachten. Da ich im dritten Byte meiner Subnetzmaske den Wert 224 notiert habe, werden die ersten drei Bits des dritten Bytes der IP-Adresse zusätzlich als Bestandteil der Net-ID mit ausgewertet. Ich muss jetzt für dieses Byte der IP-Adresse Dezimalwerte finden, die in den ersten drei Bits eine identische Struktur aufweisen.

Diese stellen dann die Hosts eines Subnetzes dar. Betrachten wir folgende Tabelle:

Bit 1 – 3 der Subnetzmaske	Byte 3 der IP-Adresse (dezimal)		Byte 3 der IP-Adresse (binär)
000	Erster Host:	0	00000000
	Letzter Host:	31	00011111
001	Erster Host	32	00100000
	Letzter Host:	63	00111111
010	Erster Host:	64	01000000
	Letzter Host	95	01011111
011	Erster Host	96	01100000
	Letzter Host	127	01111111
100	Erster Host	128	10000000
	Letzter Host	159	10011111
101	Erster Host	160	10100000
	Letzter Host	191	10111111
110	Erster Host	192	11000000
	Letzter Host	223	11011111
111	Erster Host	224	11100000
	Letzter Host	255	11111111

Betrachten Sie die Tabelle genau! Trage ich in das dritte Byte meiner IP-Adresse Dezimalwerte in den Grenzen von 1 bis 31 ein, so sind alle diese Werte, betrachtet man einmal ihre binäre Repräsentation in der ersten drei Bits, identisch. Daraus folgt, dass mein erstes Subnetz folgenden Adressbereich besitzt:

1. Subnetz	172.16. 0.1 bis 172.16.31.254

Für die weiteren Subnetze gilt also analog:

2. Subnetz	172.16.32.1 – 172.16.63.254
3. Subnetz	172.16.64.1 – 172.16.95.254
4. Subnetz	172.16.96.1 – 172.16.127.254
5. Subnetz	172.16.128.1 – 172.16.159.254
6. Subnetz	172.16.160.1 – 172.16.191.254
7. Subnetz	172.16.192.1 – 172.16.223.254
8. Subnetz	172.16.224.1 – 172.16.255.254

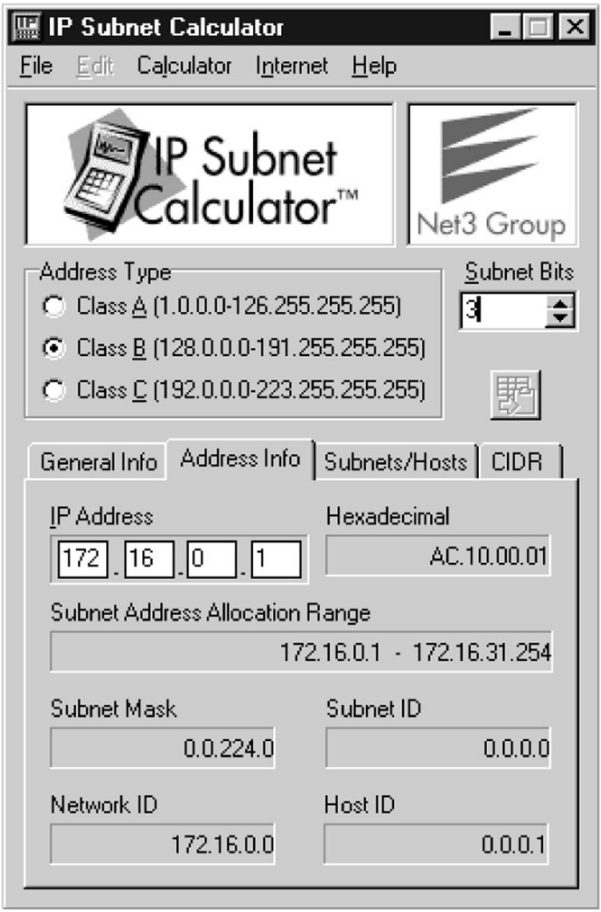
Die Schwierigkeit dieses Ansatzes besteht darin, dass wir mit dezimalen Werten arbeiten, uns aber immer wieder deren binäre Repräsentation vergegenwärtigen müssen – und das ist nicht immer ganz leicht. Belohnt werden wir aber bei diesem Ansatz mit einer flexibleren Netzwerkstruktur.

Sie werden sich jetzt sicherlich fragen: „Muss dass denn jetzt sein?“ In vielen Fällen ist es sicherlich nicht, unbedingt notwendig mit Subnetzmasken zu arbeiten z. B. bei kleinen, einfach strukturierten Netzwerken. In den meisten Fällen wird man jedoch durch die Umstände der Unternehmen dazu gezwungen, in diesem relativ komplexen Bereichen zu arbeiten. Deshalb möchte ich Ihnen noch eine kleine Software empfehlen, die mir ein Kollege ans Herz gelegt hat und die als Freeware im Internet zu beziehen ist.

Bei dieser Software handelt es sich um einen IP-Subnetz-Berechnungsprogramm. Planen Sie ein TCP/IP-Netzwerk, so berechnet Ihnen dieses Programm für die von Ihnen gewählte Netzwerkklasse bei einer gewählten Subnetzmaske die Subnetzgrößen und jeweiligen IP-Adressbereiche.

Den IP-Subnet Calculator der Firma Net3 Group laden Sie einfach von deren Homepage www.net3group.com herunter. Sie erhalten dann ein Setup-Programm, das Ihnen dabei hilft, die Software zu installieren. Das ist ein ganz einfacher Standard-Windows-Setup Dialog, der von Ihnen keine schwerwiegenden Angaben erfordert. Danach steht das Programm im Dialog Start-Programme zur Verfügung.

Hier sehen Sie das Register Address Info des IP Subnet Calculator:

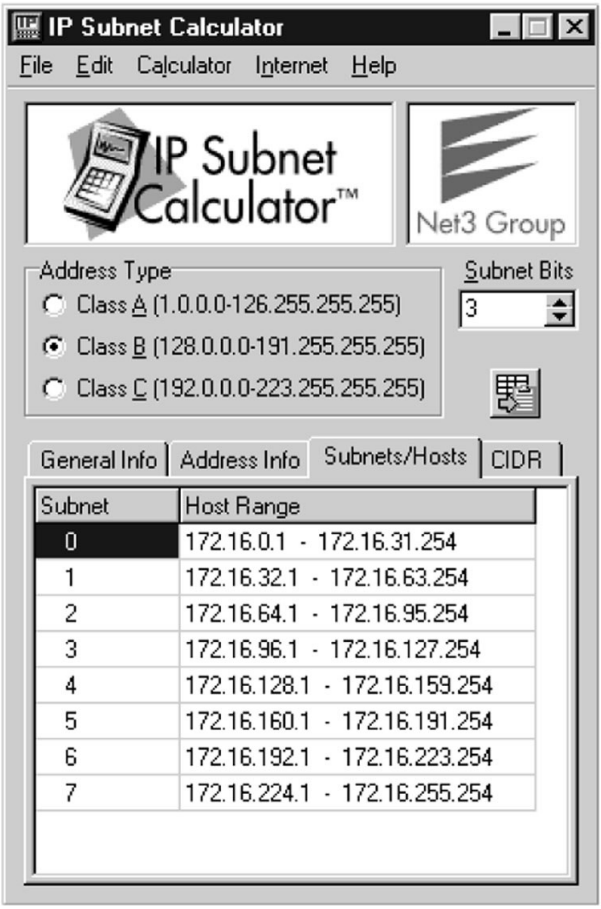


Startadresse des Netzwerks eintragen

Für die Berechnung unseres Beispielnetzwerkes habe ich die Adressklasse B markiert und in das Feld IP-Adress die Startadresse des TCP/IP-Netzwerks eingetragen. In das Feld Subnet Bits habe ich dann noch den Wert drei (3) notiert. Was bedeutet das? Meine

projektierte Subnetzmaske heißt 255.255.224.0. Im dritten Byte sehen Sie den Wert 224. Dieser Wert fragt die ersten drei (3) Bits des 3. Bytes der IP-Adresse als Net-ID ab und somit muss ich also in dieses Feld den Wert drei (3) eintragen.

Da mich die Subnetzstruktur und die Adressierungsbereiche der einzelnen Subnetze interessieren, wechsle ich in das Register Subnets/Hosts:



Register Subnets/Hosts

Sehen Sie, was wir uns vorhin mühselig durch dezimal-zu-binär-Umrechnungen erarbeitet haben, wird uns hier in Sekundenschnelle automatisch serviert. Wenn das keine Arbeitserleichterung ist!

Mit diesem theoretischen Wissen ausgestattet sollten Sie in der Lage sein, für Ihr Netzwerk IP-Adressen bereitzustellen.

5.2.4 Die AS/400 TCP/IP-Konfiguration

Seit OS/400 Version 3 Release 1 werden die TCP/IP-Protokollstapel als integrierter Bestandteil des Betriebssystems ausgeliefert. Dieses bedeutet jedoch nicht, dass nicht vorher schon ein TCP/IP für die AS/400 verfügbar gewesen wäre. Der Unterschied zur aktuellen TCP/IP Version besteht darin, dass die Altversion ausschließlich als Lizenzprogramm zur Verfügung stand, damit natürlich kostenpflichtig war, und dass das TCP/IP im Userinterface des Betriebssystems funktional tätig war, was dazu führte, dass TCP/IP-Verbindungen weniger performand waren als SNA-Verbindungen. Dieses Gründe insgesamt waren die Ursache, dass TCP/IP-Verbindungen auf der AS/400 nicht sonderlich beliebt waren.

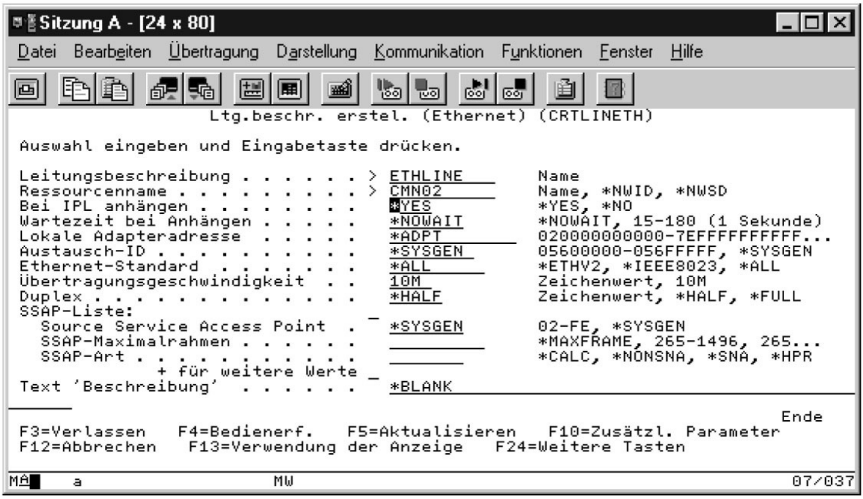
Die aktuelle TCP/IP-Implementierung ist von den eben genannten Merkmalen frei. Das TCP/IP ist in das Betriebssystem integriert, d. h. seine Funktionen sind weitgehend in den Microcode des OS/400 eingebracht worden, was zur Stabilität und Schnelligkeit dieser Verbindungsmöglichkeit erheblich beitrug.

5.2.4.1 Lokale Netzwerke

Voraussetzung für eine lokale Verbindung mit Hilfe des TCP/IP-Protokolls ist das Vorhandensein einer physischen Leitung – Ethernet oder Token Ring.

5.2.4.1.1 Ethernet Netzwerke

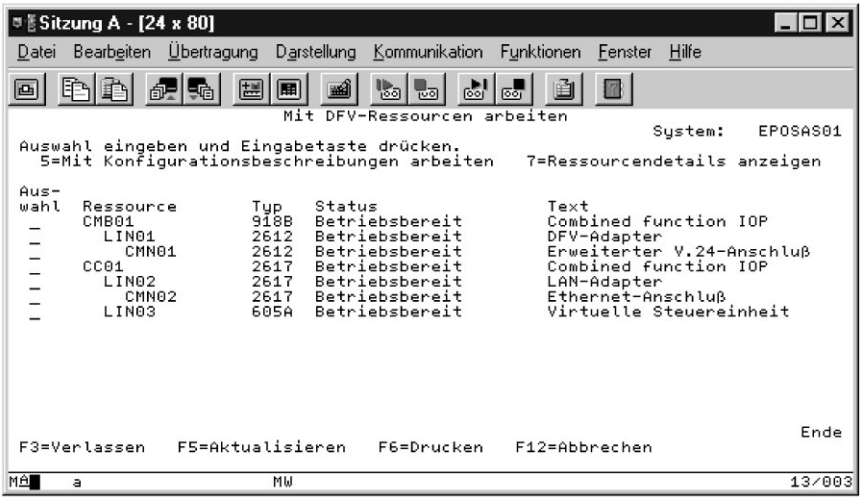
Im Folgenden sehen Sie eine typische Ethernet-Leitungsbeschreibung. Welche Parameter sind wichtig?



Ethernet Leitungsbeschreibung

Name der Leitung
frei wählbar

Ressourcenname
Mit Hilfe der Anzeige des Befehl WRKHDWRSC (Mit Hardwareressourcen arbeiten) ermitteln Sie den Ressourcennamen der LAN-Adapterkarte.



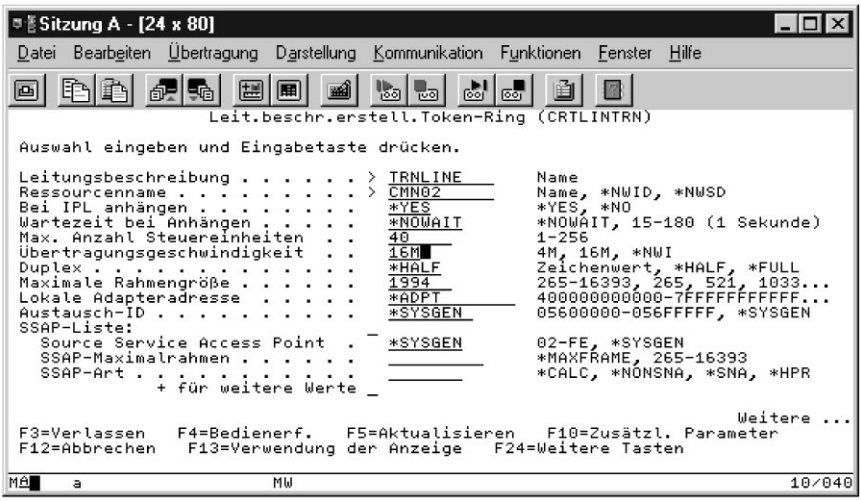
*Anzeige des Befehls WRKHDWRSC *CMN*

Adapteradresse

Die Adapteradresse wird über den Einsetzwert *SYSGEN vom System ermittelt.

5.2.4.1.2 Token Ring Netzwerke

Nachfolgend sehen Sie eine typische Token Ring-Leitungsbeschreibung. Welche Parameter sind wichtig?



Token Ring-Leitungsbeschreibung

Name der Leitung
Frei wählbar

Ressourcenname
siehe Ethernet-Adapter

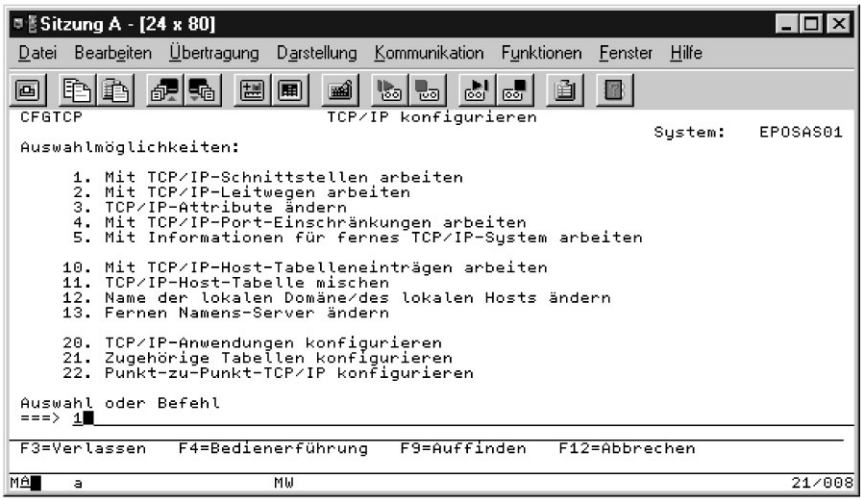
Adapteradresse
siehe Ethernet-Adapter

5.2.4.2 Erstellung einer TCP/IP Schnittstelle

Die gesamte Konfiguration der TCP/IP-Funktionen kann aus dem AS/400-Menü CFGTCP heraus erfolgen. Dieses Menü erreichen Sie auf zwei unterschiedliche Arten:

1. Geben Sie auf einer beliebigen Befehlszeile den Befehl CFGTCP (TCP/IP konfigurieren) ein.
2. Alternativ können Sie auch den direkten Menüaufruf GO CFGTCP eingeben.

Welchen der beiden genannten Wege Sie gewählt haben, ist letztendlich egal. Sie erhalten auf alle Fälle den folgenden Bildschirm als Anzeige:



Menü CFGTCP

Wählen Sie jetzt den Menüpunkt 1 (Mit TCP/IP-Schnittstellen arbeiten). Sie sehen daraufhin den folgenden Bildschirm:

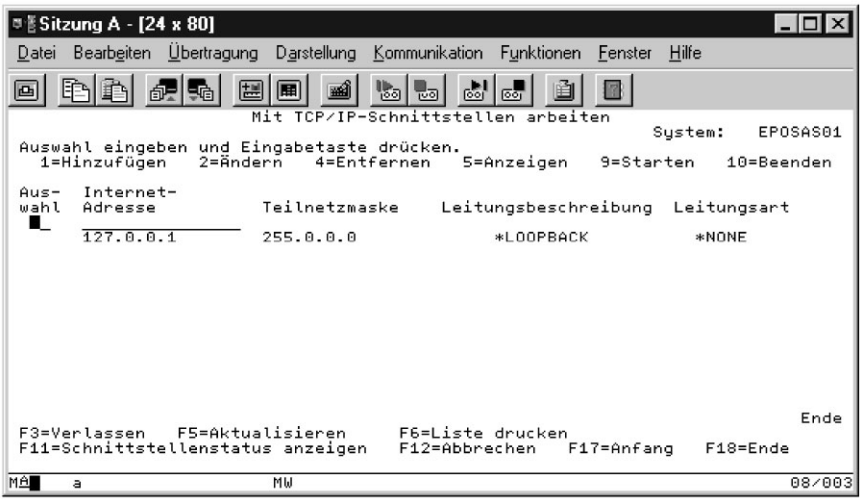
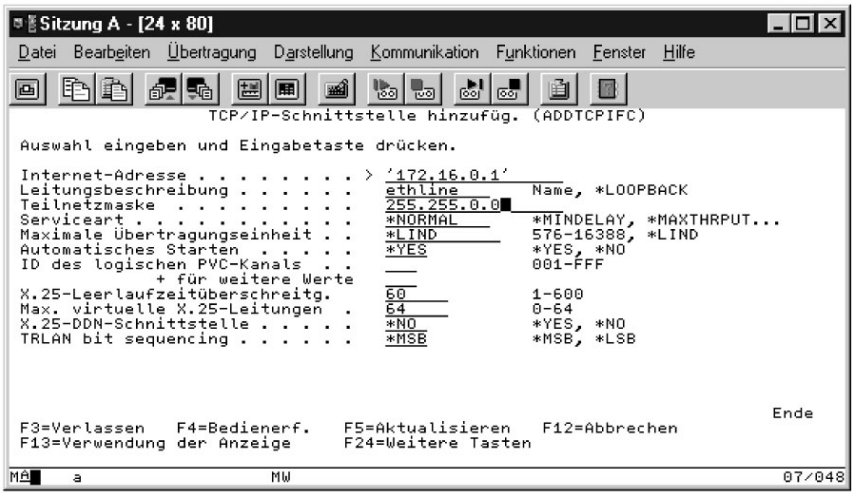


Bild: Mit TCP/IP Schnittstellen arbeiten

Worin liegt der Sinn eine TCP/IP Schnittstelle zu definieren? Es geht darum, dass Sie Ihre AS/400 in einem TCP/IP-Netzwerk adressierungsfähig machen. Das erreichen Sie dadurch, indem Sie eine TCP/IP Adresse an die Leitungsbeschreibung (Ethernet oder Token Ring) Ihrer AS/400 binden.

Sie sehen, dass bereits eine Adresse eingetragen ist. Die Adresse 127.0.0.1 ist eine sogenannte LOOPBACK Adresse, eine interne Adresse zur Überprüfung der lokalen TCP/IP-Konfiguration. Wir können aber zu diesem Zeitpunkt noch nicht prüfen, denn wir müssen ja erst einmal eine TCP/IP-Schnittstelle erstellen, bevor wir überhaupt etwas zum Prüfen haben.

Geben Sie also eine 1=Hinzufügen im Auswahlfeld, gefolgt von Ihrer selbstgewählten IP-Adresse ein, folgender Bildschirm erscheint:



TCP/IP Schnittstelle erstellen

IP-Adresse

Hier sollte jetzt Ihre eingebene IP-Adresse als Zeichenkette stehen. Im Bild sehen Sie die Zeichenfolge 172.16.0.1. Aber warum wurde die Net-ID 172.16 gewählt? Aus dem Wertebereich ergibt sich, dass es sich hier um eine Class B-Adresse handelt.

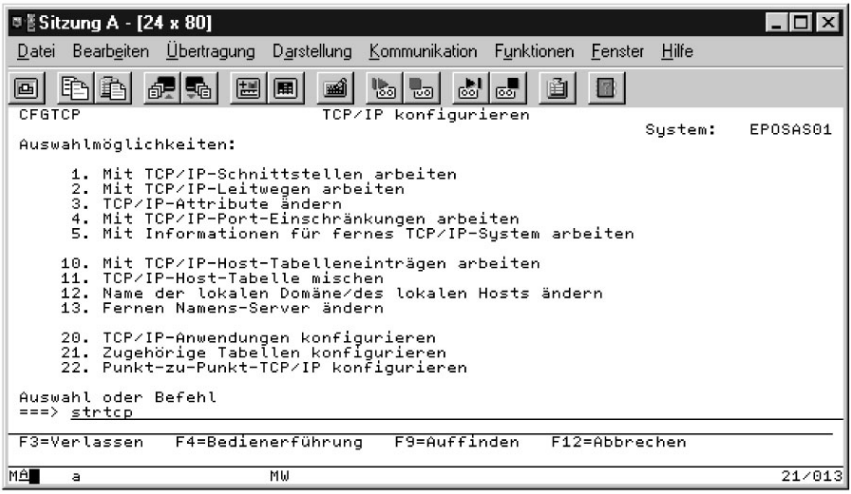
Wie Sie sehen, habe ich mich aus dem Adressenpool privater Class B-Adressen bedient. Das gibt mir die Sicherheit, sollte mein Netzwerk zum Internet hin geöffnet werden, dass ich keine bereits im Internet vergebene Adresse verwende. Darüber hinaus haben die freigelassenen Adressen den Vorteil, dass an sie kein Provider seine Dienste direkt durchrouten kann.

Leitungsbeschreibung
Als Leitungbeschreibung geben Sie die von Ihnen ausgewählte Leitung ein, über die TCP/IP-Dienste wahrgenommen werden sollen. In meinem Fall die Ethernet-Leitung ETHLINE.

Subnetzmaske
Tragen Sie hier den Wert 255.255.0.0 ein. Dieser Wert besagt, dass alle Bits des ersten und des zweiten Bytes der IP-Adresse komplett als Net-ID interpretiert werden.

5.2.4.3 Die TCP/IP Schnittstelle starten

Geben Sie jetzt den Befehl STRTCP ein.



STRTCP

Dieser Befehl kann eine Reihe von TCP/IP Diensten starten. Welche der im Folgenden aufgeführten Dienste gestartet wird, ist bei der Einzelkonfiguration auf Dienstebene festgelegt.

FTP:	File Transfer Protocol – einfacher Dateitransfer
TELNET:	Bildschirmemulation
SMTP:	E-Mail-Protokoll
POP3:	Post Office-Server
HTTP:	Internet-Server
WSG:	Workstation-Gateway

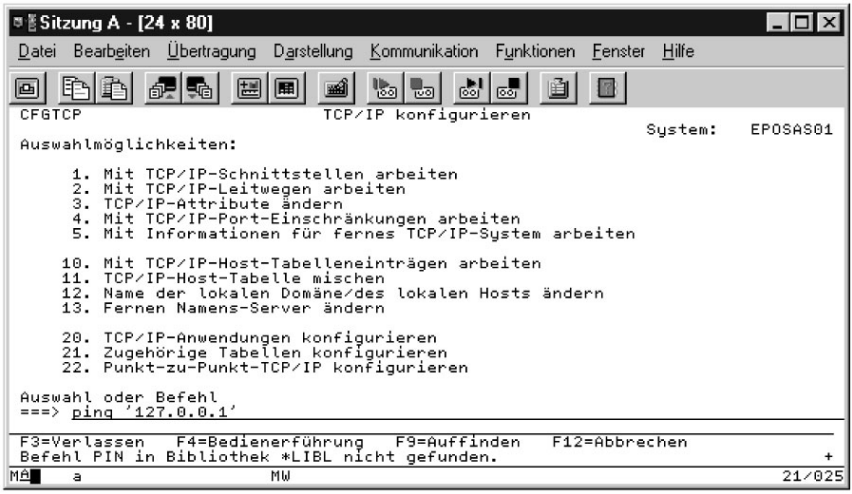
Wir gehen jetzt in den Befehl WRKACTJOB und sehen uns im Subsystem QSYSWRK die TCP/IP-Jobaktivitäten an. Folgende Jobs sind u. a. bei kompletter TCP/IP-Dienstkonfiguration sichtbar:

QTCPIP	TCP/IP-Masterjob
QTFTPxxxxx	FTP-Funktionen
QTGTELNETS	Telnet-Funktionen
QTHTTxxxxx	Internet-Server Funktionen
QTLPDxxxxx	Line Printer Daemon – Funktionen
QTSNMPxxx	Simple Network Management Protocol – Funktionen
QTPOCxxxxx	POP3 – Server Funktionen
QTPOPxxxxx	weitere POP3 – Server Funktionen
QTSMTPxxxx	Simple Mail Transport Protocol – Funktionen
QTWSGxxxxx	Workstation Gateway – Funktionen

5.2.4.4 Die Funktion der TCP/IP Schnittstelle überprüfen

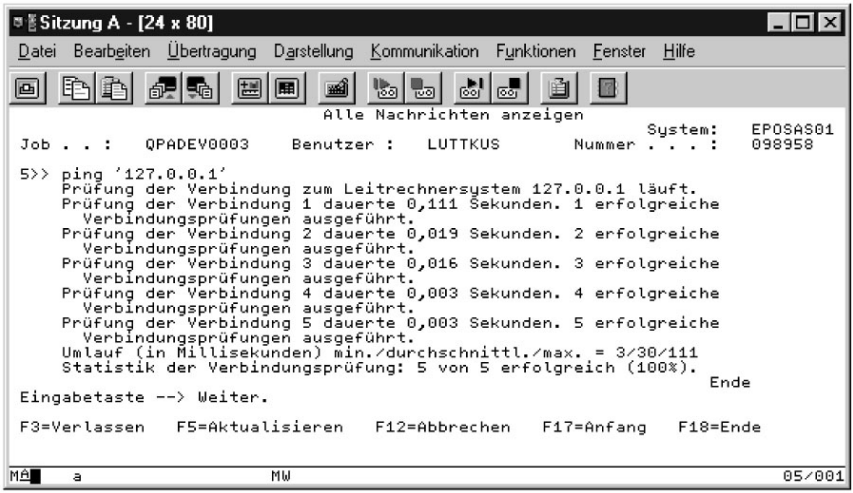
Soweit scheint alles gut gelaufen zu sein. Aber wir brauchen noch ein handfestes Prüfungsergebnis, ob unsere Schnittstelle auch wirklich betriebsbereit ist.

Geben Sie den Befehl PING ein, gefolgt von der LOOPBACK Adresse 127.0.0.1.



Prüfen der Konfiguration: PING ‚127.0.0.1'

Folgende Meldungen sollten in der Statuszeile des Bildschirms erscheinen:



PING Meldungen: Erfolg – die Konfiguration steht!

5.2.4.4.1 Troubleshooting

Dieses Mal haben wir eine Schnittstelle erfolgreich erstellt. Welche Prüfschritte sind aber für den Fall eines Fehlers zu durchlaufen?

1. **Überprüfung der physikalischen Schnittstelle – Leitungsbeschreibung**

Jedes TCP/IP-Paket, das von Ihrer AS/400 empfangen werden soll, muss einen Prüfprozess durchlaufen, der das Paketierungsformat dieses Pakets überprüft. Dieser Prüfvorgang wird über

einen sogenannten Source Service Access Point (SSAP) gesteuert, der mit einer zweistelligen hexnumerischen Adresse benannt wird. Diesen Parameter finden Sie im Rahmen einer SSAP-Liste in der Leitungsbeschreibung:

```
SSAP-Liste:
   Source Service Access Point  .   04
   SSAP-Maximalrahmen . . . . . .   1496
   SSAP-Art . . . . . . . . . . .   *SNA

   Source Service Access Point  .   12
   SSAP-Maximalrahmen . . . . . .   1496
   SSAP-Art . . . . . . . . . . .   *NONSNA

   Source Service Access Point  .   AA
   SSAP-Maximalrahmen . . . . . .   1496
   SSAP-Art . . . . . . . . . . .   *NONSNA
```

Der für die Überprüfung von TCP/IP-Paketen zuständige SSAP trägt die Adresse AA. Sollte dieser SSAP nicht vorhanden sein, so kann keine TCP/IP-Kommunikation stattfinden.

2. Überprüfung der TCP/IP Serverjobs

Die logische TCP/IP-Schnittstelle kann nur erfolgreich aktiviert werden, wenn das Subsystem QSYSWRK erfolgreich gestartet wurde. In den allermeisten Fällen wird der STRTCP-Befehl durch das Systemstartprogramm der AS/400 – QSTRUP – ausgeführt. Können Sie die Schnittstelle zwar selbst starten, jedoch nicht aus dem Startprogramm heraus, so sind zwei Ursachen typisch:

– Sie haben den Befehl STRTCP im Startprogramm nicht an das Ende gestellt, sondern eher in der Mitte plaziert. Da das Startprogramm den Start der Subsysteme einleitet, jedoch das Ende des Vorgangs nicht abwartet, sondern weiterläuft, ist es mehr als wahrscheinlich, dass das Subsystem QSYSRWK noch nicht komplett gestartet wurde, so dass der Job QTCPIP, der die Schnitt-stellenfunktion darstellt, nicht gestartet werden konnte.

Plazieren Sie den Aufruf von STRTCP ganz ans Ende des Programms QSTRUP. Sollte das nicht ausreichen, so kodieren Sie vor den STRTCP-Befehl einen DLYJOB (Zeitverzögerung für Job) von 30 bis 60 Sekunden.

– Möglicherweise ist der Befehl STRTCP berechtigungstechnisch so geschützt, dass das Programm QSTRUP nicht das Recht hat, diesen Befehl auszuführen. QSTRUP läuft als Standard unter dem Benutzer QPGMR. Sollte dieser Benutzer nicht das Recht haben STRTCP auszuführen, sollten Sie QPGMR das *USE Recht für den Befehl erteilen.

3. Überprüfen der TCP/IP Adressen

Befinden sich die Adressen der zu verbindenden Host im gleichen logischen Netzwerk?

– Überprüfen Sie die Net-ID der Adresse auf Gleichheit.

– Überprüfen Sie die Subnetzmaske auf Gleichheit.

5.2.2.5 Die Host Tabelle

Stellen Sie sich einmal vor, dass Sie nicht nur ein, zwei, fünf oder zehn Systeme TCP/IP-fähig machen müssen, sondern summa summarum 200 oder 300 oder 500 oder … Es wird Ihnen jetzt sicher nicht schwerfallen, diese Anzahl von Adressen zu generieren, aber wenn es jetzt zu Fehlern in Ihrem Netzwerk kommt und Sie erhalten Meldungen zum System 172.16.233.52 oder 172.16.188.47, so werden Sie sicher Schwierigkeiten haben, sich zu erinnern, wo und an welchem Arbeitsplatz diese Systeme zu finden sind. Also wäre es doch schön, wenn es die Möglichkeit gebe, „richtige“ Namen für die Systeme zu vergeben. Diese Namen sollen es Ihnen ermöglichen, ein bestimmtes System genau zu lokalisieren.

Diese Möglichkeit wird Ihnen mit der Host-Tabelle gegeben. Eine Host Tabelle ist ein lokales Objekt, welches auf jedem TCP/IP-Host implementiert werden kann und einer numerischen TCP/IP Adresse eine verbale Adresse zuordnet.

Rufen Sie im Menü CFGTCP den Punkt 10 (Mit TCP/IP-Host Tabelleneinträgen arbeiten) auf. Es erscheint auf der AS/400 folgenden Anzeige:

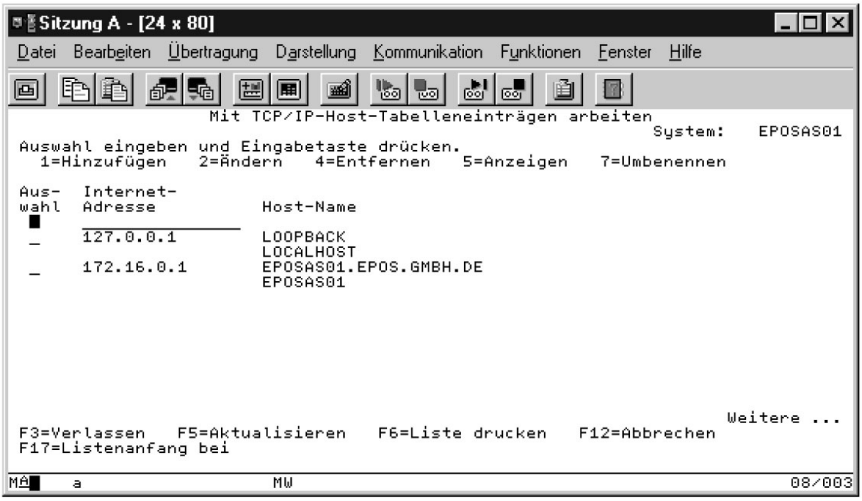
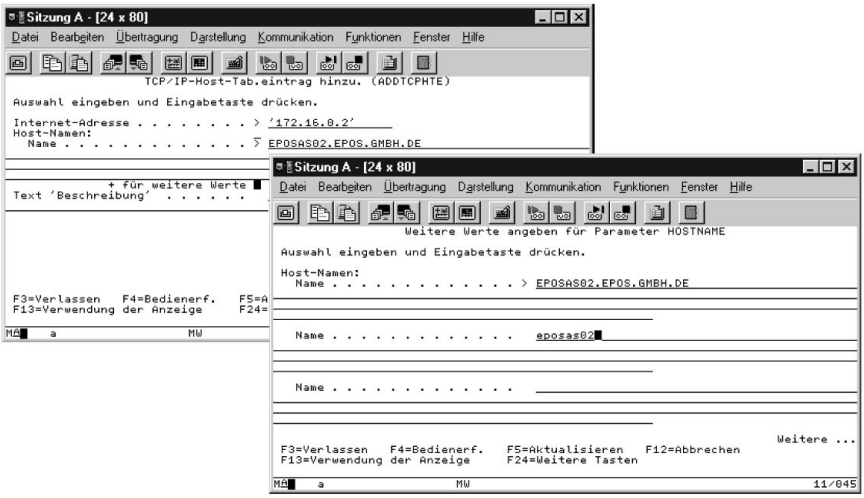


Bild: Mit Host-Tabellen arbeiten

Ich werde jetzt eine zweite AS/400, Systemname EPOSAS02, mit einem sprechenden Namen ansprechen.

Ich wähle also 1=Hinzufügen und gebe folgende Werte ein:



Host-Tabelleneintrag erfassen

Wie Sie leicht erkennen können, vergebe ich zwei Namen. Der erste Name ‚EPOSAS02.EPOS.GMBH.DE, wird der IP-Adresse direkt zugeordnet. Der zweite Name, EPOSAS02, ist als Alias-Name hinterlegt und wird generell für Schreibfaule vorgehalten. PING EPOSAS02 gibt sich doch schneller ein als PING EPOSAS02.EPOSGMBH.DE, oder?

5.3 Windows-TCP/IP

Die Windows-TCP/IP-Konfiguration wird ausschließlich aus dem Netzwerk-Setup heraus erledigt. Die derzeit gängigen Windows-Versionen haben alle ähnliche Setup-Dialoge, die ich im Folgenden kurz erläutern werde.

5.3.1 Windows for Workgroups-TCP/IP

Bevor Sie die TCP/IP-Stacks für Windows for Workgroups installieren können, gibt es eine kleine Schwierigkeit: TCP/IP gehört nicht zum Auslieferungsumfang von Windows for Workgroups!

Hieran schließen sich weitere, wenn auch kleine Probleme an:

1. Welches ist der richtige TCP/IP-Protokoll-Stack?
2. Wie erlangen Sie in den Besitz des entsprechenden Protokoll-Stacks?

Lösung von Problem 1:

Von Microsoft werden mehrere TCP/IP-Stacks ausgeliefert, der für unseren Zweck richtige heißt: MS TCP/IP-32 3.11b.

Lösung von Problem 2:

Falls Sie einen Internetzugang haben, sollten Sie auf die Treiber Download-Homepage der Firma Microsoft gehen und den oben genannten TCP/IP-Stack auf Ihr System herunterladen.

Eine weitere Möglichkeit, die Windows TCP/IP-Stacks zu bekommen, besteht darin, dass Sie sich den Zugang zur Windows

NT 4.0 Server CD beschaffen. Auf dieser CD gibt es folgenden Verzeichnispfad:

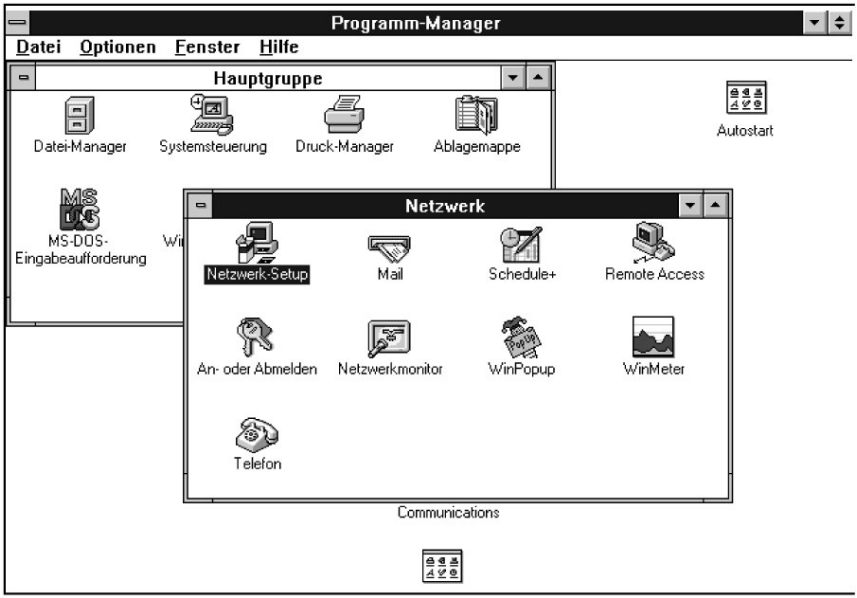
\clients\tcp32wfw\disks\disk1

Kopieren Sie den gesamten Inhalt dieses Verzeichnisses auf eine Diskette oder in ein Netzwerkverzeichnis und rufen Sie dann von dort die Setup-Routine auf.

Nachdem Sie diese Probleme gelöst haben, kann TCP/IP (endlich) auf Ihrem Windows for Workgroups-System installiert und konfiguriert werden

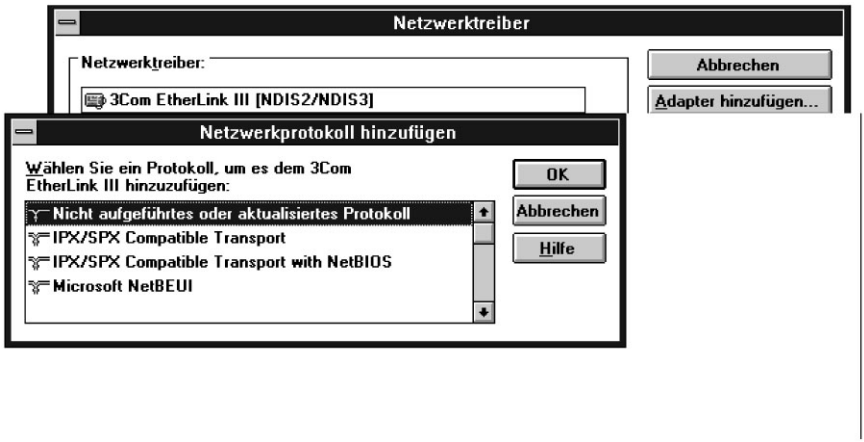
5.3.1.1 Windows for Workgroups-TCP/IP installieren

Gehen wir davon aus, dass Sie Ihren TCP/IP-Stack auf eine Diskette kopiert haben. Die Diskette befindet sich in Laufwerk A: Ihres PCs.

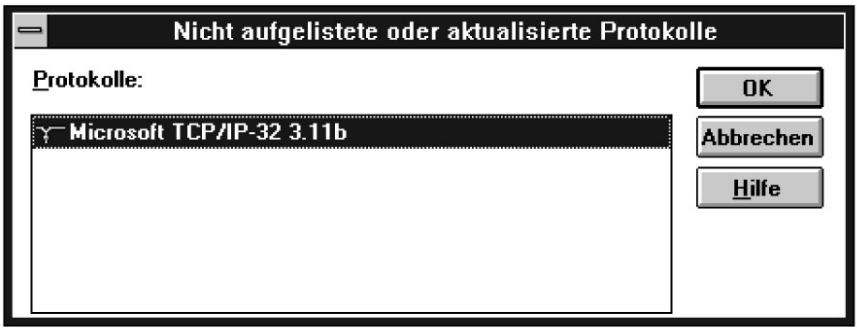


Programmgruppe Netzwerk

Drücken Sie im Netzwerksetup den Button Treiber und folgender Bildschirm erscheint:

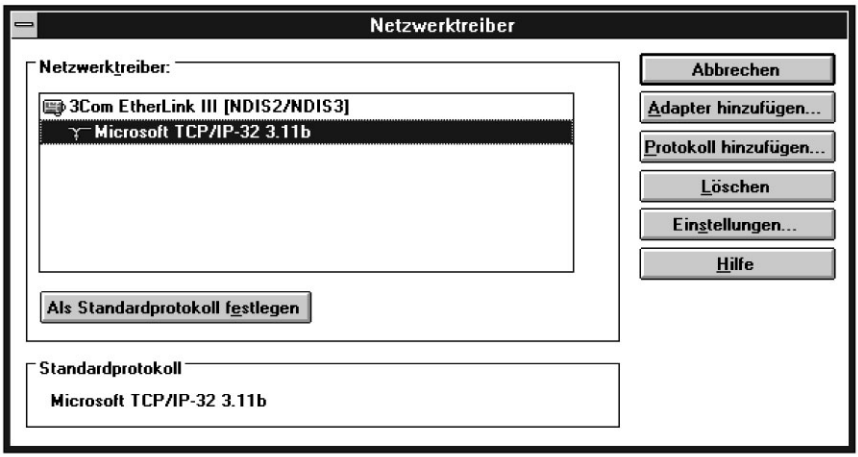


Wählen Sie hier den Button „Protokoll hinzufügen“ und markieren Sie die Auswahl „Nicht aufgeführtes oder aktualisiertes Protokoll“. Legen Sie die von Ihnen erstellte TCP/IP-Diskette ins Laufwerk ein. Folgendes Fenster wird abgebildet:



Jetzt wird der TCP/IP-Protokollstapel auf Ihren PC kopiert.

Danach sollten Ihre Netzwerkattribute wie folgt aussehen:



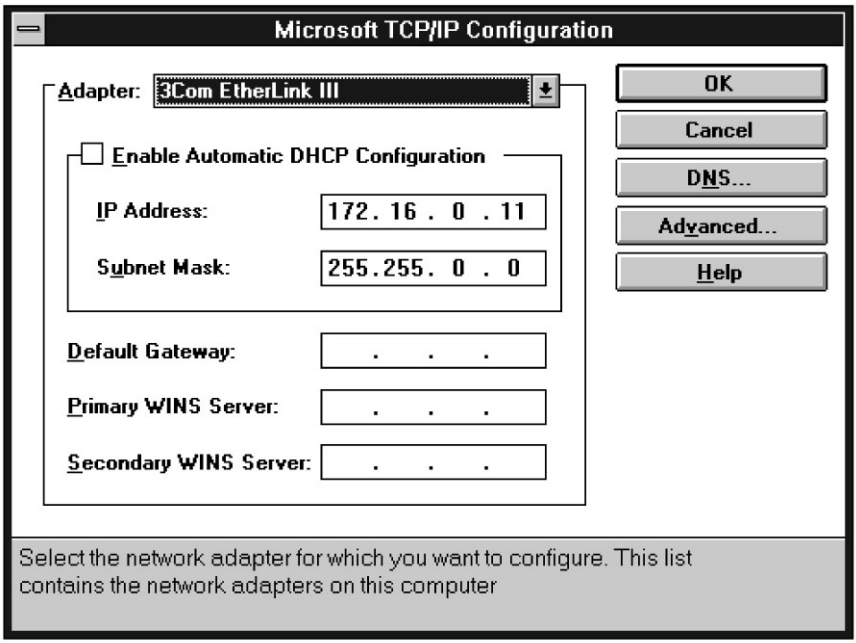
Der TCP/IP-Stack ist als Standardprotokoll festgelegt worden.

Markieren Sie das von Ihnen installierte Protokoll. Mit Hilfe des Buttons „Einstellungen ...“ wird dann TCP/IP konfiguriert.

5.3.1.2 Windows for Workgroups-TCP/IP konfigurieren

Gehen Sie zuerst in der Programmgruppe Netzwerk in das Netzwerk-Setup.

Vergeben Sie eine Festgelegte IP-Adresse



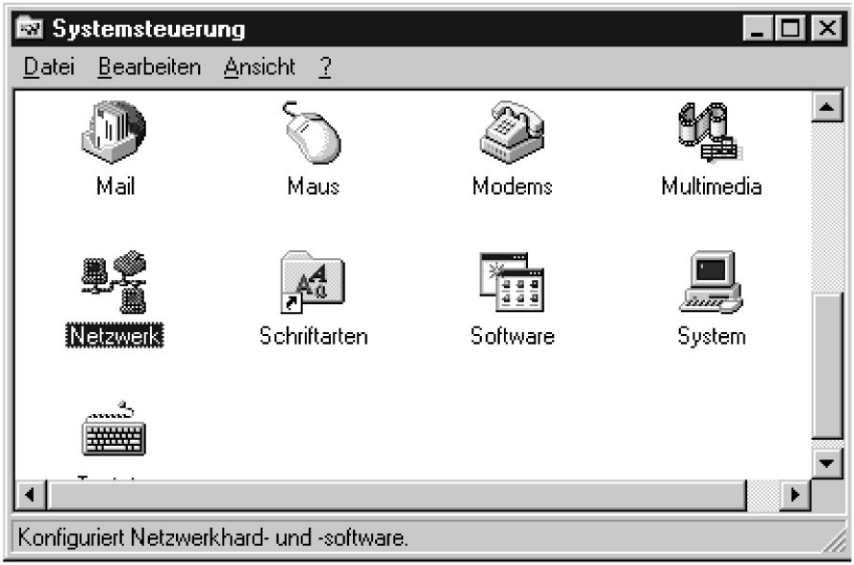
Starten Sie Ihren Windows for Workgroups-PC und die TCP/IP-Konfiguration ist beendet.

5.3.2 Windows 95-TCP/IP

Bei Windows 95, Version A und Version B, werden die Microsoft TCP/IP-Stacks als Bestandteil des Betriebssystems ausgeliefert. Die gesamte Installation und Konfiguration erfolgt in der Windows 95-Systemsteuerung im Dialog „Netzwerk“.

5.3.2.1 Windows 95-TCP/IP installieren

Sie befinden sich auf dem Desktop Ihres Windows 95 PCs. Betätigen Sie jetzt den Start-Button in der Startleiste und wählen Sie die Menüpunkte Einstellungen, Systemsteuerung. Es öffnet sich die Programmgruppe „Systemsteuerung“.



Die Programmgruppe „Systemsteuerung“

Klicken Sie jetzt auf das Icon Netzwerk und der Netzwerkinstallationsdialog beginnt.

Dialog Netzwerk

Aufgrund der Plug'n Play-Funktionalität ist die von Ihnen installierte Netzwerkkarte automatisch erkannt worden.

Falls nicht, muss der von Ihnen gewählte Adapter ein wirklich altes Schätzchen sein. Es bedeutet jedoch nicht, dass Sie die Konfiguration abbrechen müssen. Besitzen Sie eine vom Hersteller der Karte mitgelieferte Adaptertreiberdiskette für Windows 95, so müssen Sie sich dem Installationsdialog dieser Diskette anvertrauen und die Chancen sind gut, dass Sie Erfolg haben werden.

Besitzen Sie keine Installationsdiskette und ordnet Windows 95 Ihrer Adapterkarte einen generischen Treiber zu, werden die Chancen auf einen Erfolg zwar geringer, aber nicht unmöglich.

Erkennt Windows 95 die Netzwerkkarte jedoch nicht, es wird kein generischer Treiber zugeordnet und Sie besitzen keine Installationsdisketten, dann sieht es insgesamt für eine erfolgreiche Installation des TCP/IP-Stacks schlecht aus.

Ich gehe davon aus, dass die von Ihnen gewählte Netzwerkkarte erkannt wird. Folgende Netzwerkeigenschaften werden angezeigt.

Client: Client für Microsoft-Netzwerk, andere Clients, wie z. B. der Netware-Client sind möglich, falls Sie bereits ein Novell-Netzwerk installiert haben.

Netzwerkkarte: hier eine 3COM-Ethernet-Karte

Protokoll: NETBEUI, TCP/IP und andere Protokolle, wie IPC/SPX sind möglich, falls sie sich bereits in einer Novell-Umgebung befinden

Welches ist der Start-Client des PCs? An dieser Stelle wird letztendlich gefragt, wer die Anmeldebestätigung ausführen soll.

Windows-Anmeldung: Lokale Anmeldung auf Ihrem PC, keine Bestätigung der Anmeldung durch einen Netzwerkserver.

Microsoft Client: Ein Windows NT-Server führt die Überprüfung und Bestätigung der Anmeldung durch.

Netware Client: Ein Novell Netware-Server führt die Überprüfung und Bestätigung der Anmeldung durch.

Soll Ihr PC direkt mit der AS/400 kommunizieren, ohne dass ein PC-Server beteiligt ist wählen Sie an dieser Stelle die Windows Anmeldung.

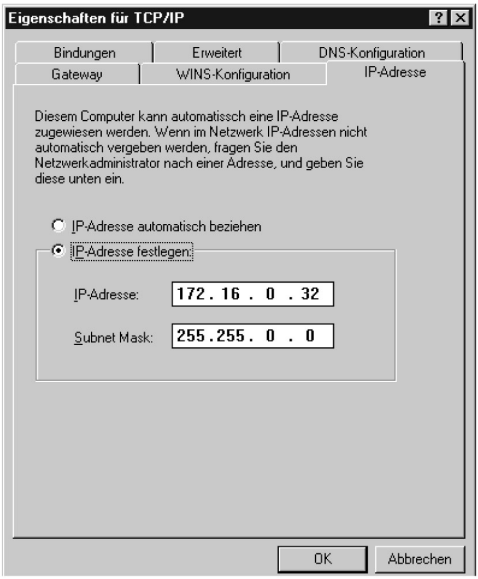
Betätigen Sie jetzt den Button „Hinzufügen“, wählen Sie „Protokolle, Microsoft, TCP/IP“ aus.

Microsoft-TCP/IP wählen

Damit ist die Installation des TCP/IP-Protokolls abgeschlossen.

5.3.2.2 Windows 95-TCP/IP konfigurieren

Ordnen Sie jetzt Ihrem PC eine IP-Adresse zu, indem Sie das TCP/IP-Protokoll doppelt anklicken.



Eine Festgelegte Adresse vergeben

Sie sehen im gezeigten Dialog, dass dem Windows 95-PC eine feste Adresse zugeordnet wurde 172.16.0.31. Er gehört damit zum gleichen logischen Netzwerk, wie die bereits konfigurierte AS/400. Auch die Subnetzmaske 255.255.0.0 wurde genauso wie auf der AS/400 vergeben. Weitere Eingaben sind nicht notwendig.

Nachdem alle Angaben mit OK bestätigt wurden, fordert Windows 95 Sie auf, die Windows 95 Installations-CD oder Disketten einzulegen und die Installation/Konfiguration wird beendet. Nach dem Neustart des PCs ist das TCP/IP Protokoll aktiv.

5.3.4 Die Datei HOSTS – die Windows Host-Tabelle

Auch der Windows-PC kennt eine Host-Tabelle. Diese ist eine einfache Textdatei mit dem Namen HOST. Diese Datei darf über keine Namenserweiterung wie .TXT, .SAM etc. verfügen.

Sie sehen in dieser Datei zwei Einträge für die Selbstprüfung der TCP/IP-Konfiguration auf diesem PC. Der Wert localhost ist der im Windows gebräuchliche Standardwert, loopback nur ein von mir vergebener Alias-Name, um mit der gleichen Syntax, wie auf der AS/400 arbeiten zu können.

Darauf folgen die Hosttabelleneinträge für die beiden bereits konfigurierten Systeme AS/400.

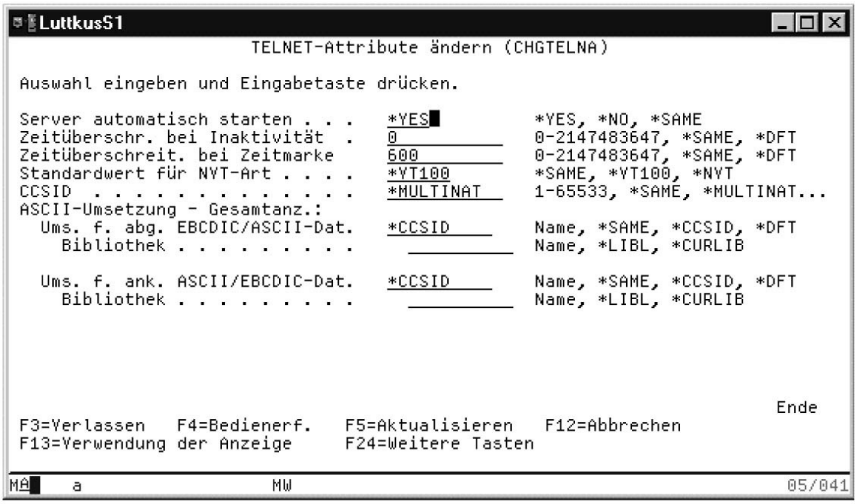
5.4 Die AS/400 TCP/IP-Funktionen

5.4.1 Telnet – die Bildschirmemulation des TCP/IPs

Für die meisten AS/400-Anwender ist der Begriff der Bildschirmemulation gleichbedeutend mit Produktnamen wie IBM Client Access, Netsoft Elite, Attachmate Rally, BOS usw., usw. Die meisten dieser Produkte verwenden in irgendeiner Form ein verbindungsherstellendes Programm, daß allgemein als Router oder als Verbindungsmanager bezeichnet wird und dessen Sinn darin besteht, während der AS/400-Kommunikation eine Verbindung zwischen der Client- und der Server-Komponente herzustellen. Aber es geht auch anders! Bestandteil der TCP/IP-Implementierung ist das sogenannte Telnet, eine Bildschirmemulation, die dem nach einfachen, schlanken und problemfreien Lösungen strebenden AS/400-Administrator weiterhelfen kann.

Telnet ermöglicht zwei unterschiedliche Arten der Bildschirmemulation: Erstens kann mit Telnet eine Bildschirmemulation zwischen zwei AS/400-Systemen aufgebaut und zweitens von einem PC- oder UNIX-Client eine Bildschirmsitzung zu einer AS/400 realisiert werden. Damit Telnet auf und für die AS/400 funktioniert, muß der sogenannte Telnetserver auf der AS/400 konfiguriert und gestartet werden.

Sie leiten die Konfiguration ein, indem Sie den Befehl CHGTELNA (Telnet-Attribute ändern) eingeben und die F4-Taste drücken.



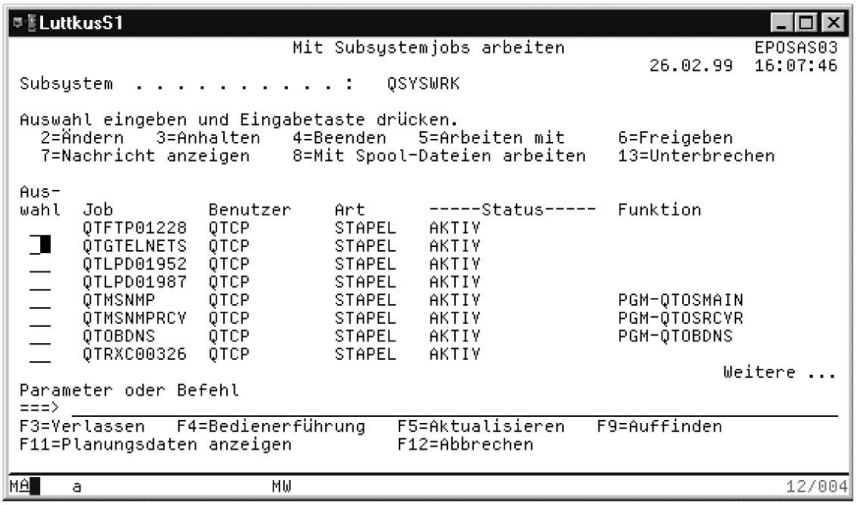
Die Attribute des Telnetservers der AS/400

Grundsätzlich muß hier keiner der Default-Parameter geändert werden, da alle eingesetzten Werte bereits die Funktion des Telnetservers ermöglichen. Ich habe hier jedoch den Parameter „Server automatisch starten“ auf *Yes gesetzt. Diese Einstellung bedingt, daß der Telnetserver mit jedem Aufruf des Befehls STRTCP automatisch gestartet wird. Sollte der Server händisch gestartet werden, so rufen Sie dazu den Befehl STRTCPSVR *TELNET auf. Soll der Telnetserver beendet werden, so rufen Sie einfach den Befehl ENDTCPSVR *TELNET auf. Ist der Telnetserver gestartet worden, so werden Sie im Subsystem QSYSWRK den Job QTGTELNETS sehen.

Rufen Sie einfach den Befehl WRKSBSJOB (mit Subsystemjobs arbeiten) folgendermaßen auf:

WRKSBSJOB QSYSWRK

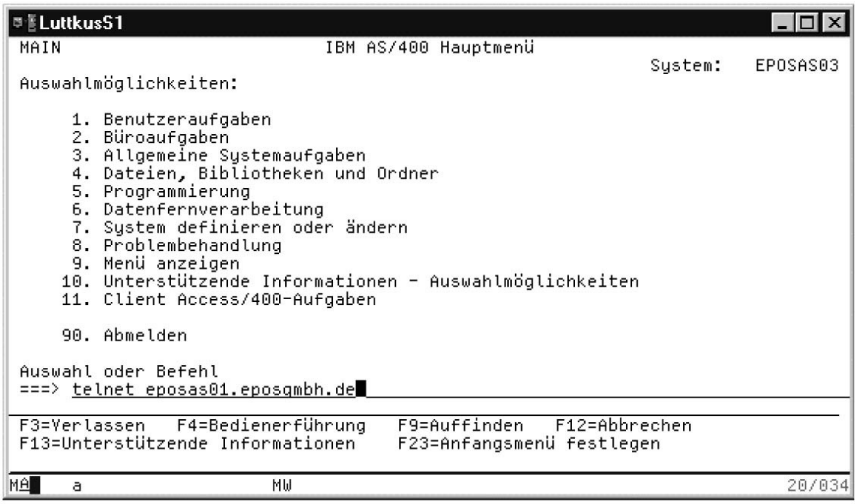
In der Anzeige sehen Sie dann die im Subsystem QSYSWRK aktiven Jobs.



Der Telnetserver ist aktiv

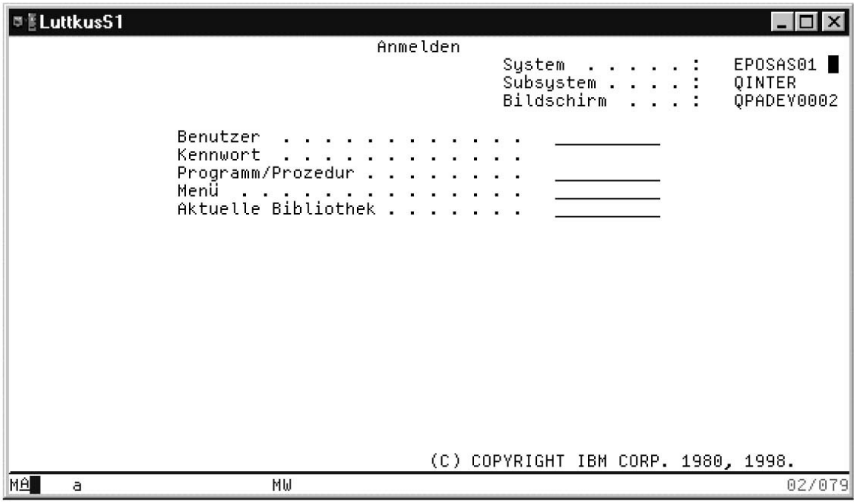
5.4.1.1 TELNET von AS/400 zur AS/400

Der Aufruf einer Telnet-Sitzung ist einfach. Voraussetzung ist eine fehlerfreie und funktionsfähige TCP/IP-Installation und -Konfiguration. Gehen wir von folgendem Beispiel aus: Wir haben zwei AS/400-Systeme; das System EPOSAS01.EPOSGMBH.DE mit der IP-Adresse 172.16.0.1 und System EPOSAS03.EPOSGMBH.DE mit der IP-Adresse 172.16.0.3. Nun wollen wir eine Telnet-Sitzung von EPOSAS03 zu EPOSAS01 herstellen. Nichts einfacher als das! Wir geben einfach den Befehl TELNET 172.16.0.1 auf der Befehlszeile des System EPOSAS03 ein. Alternativ könnten wir auch den Host-Namen des Zielsystems verwenden und folgenden Befehl eingeben: TELNET EPOSAS01.EPOSGMBH.DE.

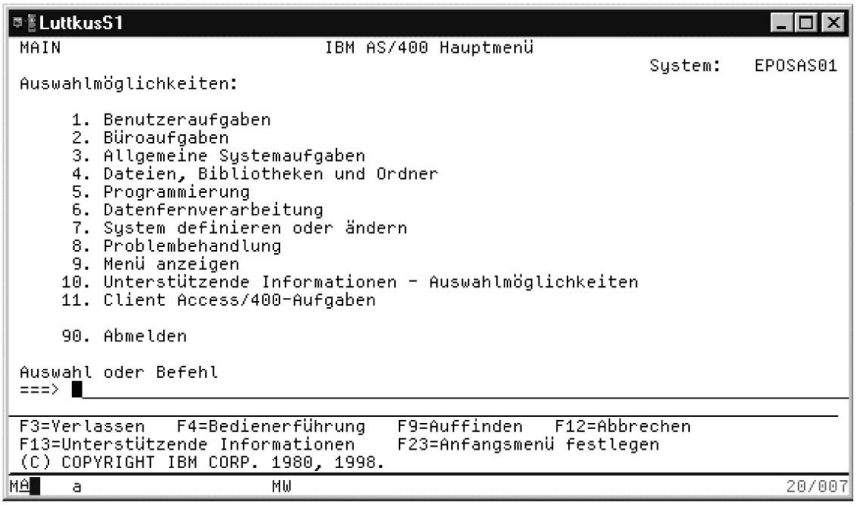


Die Telnet-Sitzung aufrufen

Danach sehen wir den Anmeldungsbildschirm des Zielsystems.



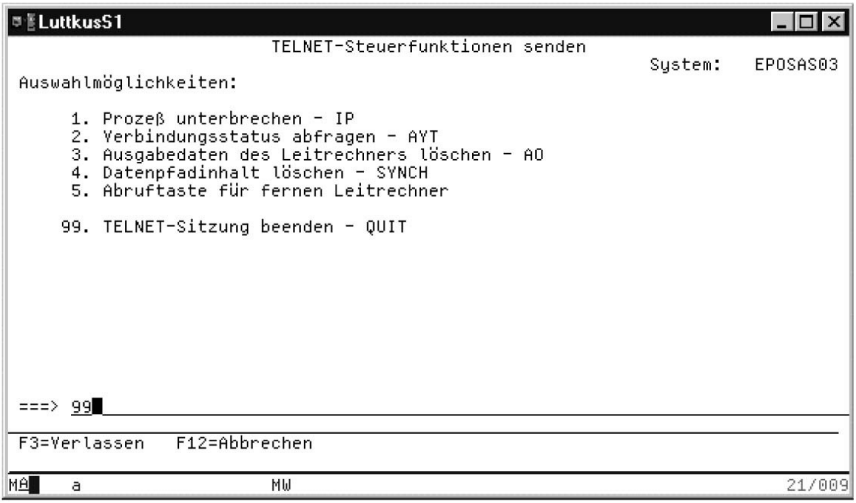
Der Anmeldungsbildschirm des Zielsystems



Nach der Anmeldung

Dieser Bildschirm unterscheidet sich durch nichts von einem „normalen“ Bildschirm. Alle Funktionstasten und Bildschirmattribute werden korrekt umgesetzt und dargestellt. Soll die Bildschirmsitzung zum fernen System beendet werden, so gibt es zwei Möglichkeiten.

1. Sie betätigen die Abruftaste. Daraufhin wird ein Beendungsmenü angezeigt.



Telnet-Sitzung beenden

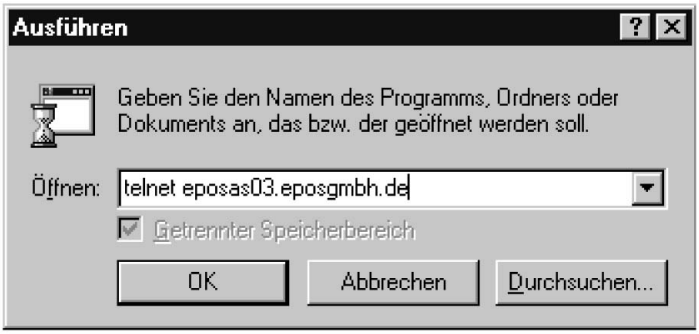
Hier wählen Sie den Menüpunkt 99 (Telnet-Sitzung beenden).

2. Sie beenden die Telnet-Sitzung, indem Sie den Befehl SIGNOFF ENDCNN(*YES) auf der Befehlszeile des Bildschirms eingeben. Auch dann wird die Bildschirmsitzung beendet.

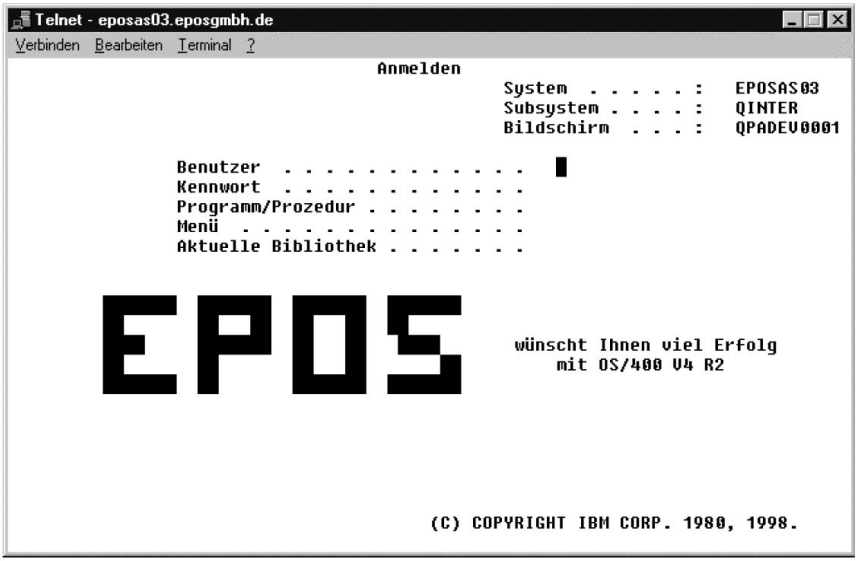
5.4.1.2 Telnet vom Windows-PC zur AS/400

Aber auch eine Telnet-Emulation vom Windows-PC zur AS/400 ist möglich. Wenden wir uns als erstes der Standard-Windows-Telnet-Variante zu. Bei ihr handelt es sich um die Emulation eines einfachen VT100-Terminals. Was heißt das? Das bedeutet rein oberflächlich betrachtet, daß einige der gewohnten 5250-Bildschirmattribute nicht wie gewohnt umgesetzt werden. Wir müssen uns daran gewöhnen, daß die Unterstriche für Eingabefelder entfallen und die Funktionstasten nicht mehr wie gewohnt funktionieren. Zwar sind die Funktionen von F1 bis F4 in beiden Terminals analog belegt, aber sonst ist alles anders. Das werden wir uns jetzt einmal ansehen. Wir gehen an unsere Windows NT Workstation – bei Windows 95 bzw. 98 sieht es ähnlich aus – und rufen aus dem Ausführen-Dialog den Befehl telnet <Zieladresse> auf.

In unsrem Beispiel verwende ich den Host-Namen EPOSAS03.EPOSGMBH.DE der angeschlossenen AS/400.



Man hätte an dieser Stelle auch hart die IP-Adresse der AS/400 eintragen können, das Ergebnis wäre dasselbe – nämlich folgender Emulationsbildschirm.



Leicht zu erkennen ist an dieser Stelle, daß die Unterstriche für Eingabefelder komplett fehlen. Das wäre sicherlich einfacher zu verschmerzen, wenn da nicht noch die Sache mit den Funktionstasten wäre. Funktionstasten dieser Emulation funktionieren fast alle anders (siehe oben). Aber keine Panik, auch in diesen Fällen sorgt die AS/400 für Abhilfe.

Wann immer Sie mit einer Telnet-Emulation auf die AS/400 zugreifen, steht für Sie ein neuer CL-Befehl zur Verfügung, der in anderen Emulationsumgebungen nicht aufgerufen werden kann. Rufen Sie den Befehl DSPVTMAP (VT-Tastenbelegung anzeigen) auf und Sie erhalten eine Darstellung der Tastaturbelegungstabelle der AS/400 für VT-Terminals.

5250-Abruftaste ..... :	*CTLA	*ESCA
Hilfe für IBM 5250 ..... :	*CTLQST	*ESCH
Bild auf (Vorwärtsblättern) ..... :	*CTLD	*CTLF
Bild ab (Rückwärtsblättern) ..... :	*CTLB	*CTLU
Systemabfrage ..... :	*CTLC	*ESCS
Einfügen ..... :	*ESCI	*ESCDLT
Löschen ..... :	*DLT	
Eingabetaste ..... :	*RETURN	
Rückschritt ..... :	*BACKSPC	
Dupliziertaste ..... :	*ESCD	
Eingabe löschen ..... :	*CTLE	
Grundstellung ..... :	*CTLR	*ESCR
Feldausgang ..... :	*CTLK	*CTLX
Feld- ..... :	*ESCM	
Pos1 ..... :	*CTLO	
Neue Zeile ..... :	*ESCLF	
Drucken ..... :	*CTLP	*ESCP

Nächstes Feld ..... :	*TAB	
Vorheriges Feld ..... :	*ESCTAB	
Cursor Auf..... :	*CSRUP	
Cursor Ab ..... :	*CSRDOWN	
Cursor Links ..... :	*CSRLEFT	
Cursor Rechts..... :	*CSRRIGHT	
Anzeige löschen ..... :	*ESCC	
Testanforderung ..... :	*CTLT	
Anzeiger umschalten..... :	*ESCT	
Anzeige wiederholen ..... :	*CTLL	
F1 ..... :	*ESC1	
F2 ..... :	*ESC2	
F ..... :	*ESC3	
F4 ..... :	*ESC4	
F5 ..... :	*ESC5	
F6 ..... :	*ESC6	
F7 ..... :	*ESC7	
F8 ..... :	*ESC8	

F9 ..... :	*ESC9	
F10 ..... :	*ESC0	
F11 ..... :	*ESCMINUS	
F12 ..... :	*ESCEQ	
F13 ..... :	*ESCEXCL	
F14 ..... :	*ESCAT	
F15 ..... :	*ESCPOUND	
F16 ..... :	*ESCDOLLAR	
F17 ..... :	*ESCPCT	
F18 ..... :	*ESCCFX	
F19 ..... :	*ESCAMP	
F20 ..... :	*ESCAST	
F21 ..... :	*ESCLPAR	
F22 ..... :	*ESCRPAR	
F23 ..... :	*ESCUS	
F24 ..... :	*ESCPLUS	

Standard-Tastaturbelegung des AS/400 VT-Terminals

Diese Tabelle erscheint auf den ersten Blick auch nicht sonderlich hilfreich, wer sich jedoch noch mit den Bildschirmen der 5150-Baureihe auskennt, wird hier doch Bekanntes entdecken. Erinnern wir uns gemeinsam. Diese alten Bildschirmterminals hatten eine Eigenschaft: Sie hatten keine Befehlstasten, wie wir es heute gewohnt sind. Um z. B. F9 zu betätigen, mußte man die sogenannte Befehlstaste drücken und dann die Zifferntaste 9. Analog funktioniert es beim VT-Terminal. Um F9 zu betätigen, drücken wir zuerst die ESC-Taste, gefolgt von der Zifferntaste 9. Man glaubt es kaum, der zuletzt eingegebene Befehl erscheint auf der nicht vorhandenen Eingabezeile des VT-Bildschirms.

Ich gebe es zu, einen derartigen Bildschirm kann man natürlich nicht einem Anwender an die Hand geben. Aber überlegen Sie einmal – der Operator, der nachts von Zuhause aus noch einmal nachsehen soll, ob auch alle Jobs normal beendet wurden, dem kann man doch einen derartigen Bildschirm zumuten. Der Vorteil ist sicherlich, daß dieses Terminal nicht annähernd so viele Ressourcen verbraucht, wie ein Client Access-Bildschirm und daß eine derartige Verbindung ausschließlich mit On-Board-Mitteln der beteiligten Betriebssysteme realisiert wird.

5.4.1.3 TN5250 – Telnet mit 5250-Attributen

Was können wir jedoch für unseren Anwender tun, der ebenfalls eine systemtechnisch einfache Bildschirmemulation benötigt? Wir können ihm eine TN5250-Emulation besorgen. Diese Form der Telnet-Emulation besticht dadurch, daß Sie das Telnet-Protokoll als Basismedium benutzt, aber alle Attribute eine 5250-Bildschirm erhält. Interessieren Sie sich für derartige Bildschirmemulationen, so sollten Sie einfach ins Internet gehen und eine der gängigen Suchmaschinen bzw. Indizes wie Yahoo.com, Lycos.com, Alta Vista.com etc. nach dem Suchbegriff TN5250 suchen lassen. Sie werden erstaunt sein, wie viele Produkte sich Ihnen anbieten. Dabei ist die Bandbreite enorm: es gibt einfache Emulationen, die als Freeware verteilt werden, anspruchsvollere Emulationen, die als Shareware vertrieben werden und große Emulationspakete, die 3270-, 5250- und VT-Emulationen in einem Produkt anbieten. Dabei wird auf die neuesten Features des TCP/IPs der AS/400 eingegangen – Vergabe von festen Bildschirmnamen, Druckeremulationen (ebenfalls mit fester Namenszuordnung), eingebaute Frontends zum FTP File-Transfer.

Als Einstieg möchte ich Ihnen folgende Home-Pages ans Herz legen:

www.sdisw.com:

Hier finden Sie ein Produkt namens TN3270plus, das Bildschirmemulationen zu 3270-, 5250- und VT-kompatiblen Systemen ermöglicht.

www.ericomm.com:

Das Produkt Powerterm Interconnect/32 ist eine komplette 3270-, VT-100 und 5250-Emulation und beinhaltet folgende Funktionen: Bildschirmemulation mit fester Namenszuordnung, Druckemulation mit fester Namenszuordnung und FTP-Filetransfer.

www.boscom.de:

Bei der Firma BOS finden Sie deren TN5250-Emulation, die alle Merkmale des TCP/IPs der AS/400 unterstützt, etwa feste Benamungen, Druckemulationen etc.

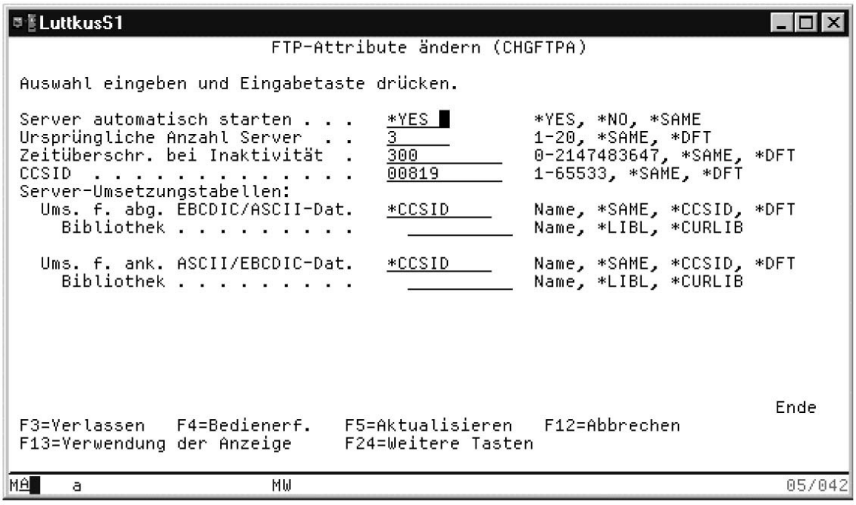
5.4.2 FTP – das File Transfer-Protokoll

FTP stellt sicherlich ähnlich wie das Telnet-Protokoll eine der sogenannten Standardfunktionen des TCP/IPs zur Verfügung. Fast jede Art von Netzwerk stellt eine Art Dateitransfer zur Verfügung. Im SNA-Netzwerk arbeiten wir mit Funktionen wie SNDNETF (Send Netfile), SNDNETSPLF (Send Net Spoolfile) etc. Diese Funktionen stellen in vielen Häusern die Grundwerkzeuge für eine robuste Datenverteilung zur Verfügung. Wenn wir dagegen die Dienste des FTPs betrachten, müssen wir von einer gänzlich anderen Situation ausgehen. Sind die SNA-Dienste nachgerade zugeschnitten auf die Fähigkeiten und Möglichkeiten, der an einem Netzwerk beteiligten IBM-Systeme, so besticht das FTP dadurch, daß es als TCP/IP-Dienst praktisch Bestandteil jeder Systemumgebung ist, die eine TCP/IP-Implementierung besitzt. Eine Folge dieser Ausgangssituation ist, das auf bestimmte systemimmanente Fähigkeiten der beteiligten Systemarchitekturen nicht eingegangen werden kann.

5.4.2.1 FTP-Server konfigurieren

Damit FTP auf einer AS/400 aktiv werden kann, muß diese Komponente des TCP/IP konfiguriert werden. Bevor wir uns jedoch an die eigentliche Konfiguration wagen, müssen zuerst einige Grundlagen geschaffen werden. Das FTP basiert auf der Funktion zweier TCP/IP-Ports – 20 und 21. Wozu zwei Ports? Der Port 21 ist der sogenannte Datenport des FTPs. Werden Daten von System A nach System B übertragen, so wird dieser Transfer über den Port 21 abgewickelt. Der Port 20 dient als sogenannter Steuerungskanal. Was heißt das? Wenn Sie System A beauftragen, Daten von System B herunterzuladen, so wird System A System B einen Befehl – in diesem Fall ein GET – übermitteln, damit der Transfer abgewickelt werden kann. Die Übergabe des Befehls erfolgt dabei über den Port 20. Übrigens wird als Transportmedium für die Befehlsübergabe ein vereinfachtes Telnet-Protokoll verwendet. Bei Funktionsstörungen des FTPs müssen beide Ports beobachtet werden.

Um FTP zu konfigurieren, geben Sie den Befehl CHGFTPA (FTP-Attribute ändern) ein und prompten Ihn mit der F4-Taste.



FTP konfigurieren

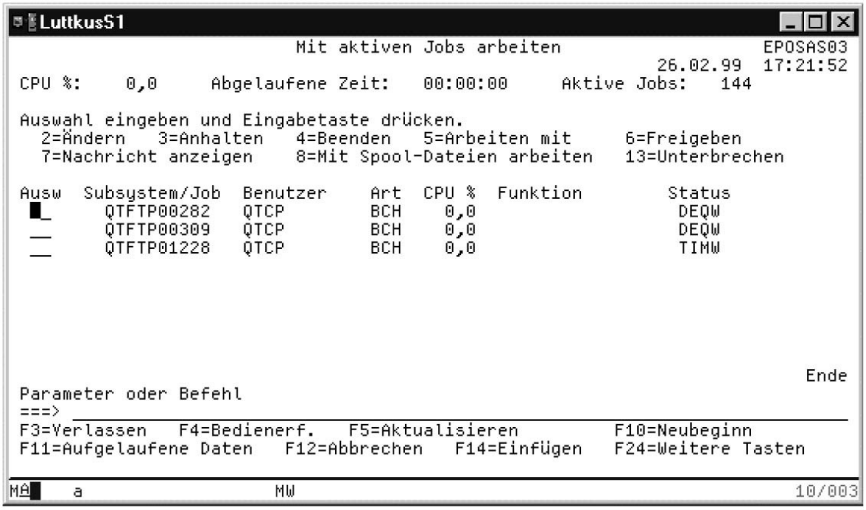
Sie sehen hier die Default-Einstellungen des AS/400-FTPs. Folgende Parameter sollten Sie beachten:

Server automatisch starten: Dieser Parameter ist auf den Wert *YES gesetzt. Dadurch werden die FTP-Server-Jobs des OS/400 mit dem Aufruf des Befehls STRTCP (TCP/IP starten) gestartet. Der Parameter „Ursprüngliche Anzahl Server“ bestimmt, wie viele der FTP-Server-Jobs gestartet werden und steht auf 3. Warum werden überhaupt mehrere Server-Jobs gestartet? Jedem FTP-Client wird beim Aufbau einer FTP-Sitzung ein eigener FTP-Server-Job zugeordnet. Trifft ein FTP-Client auf einen dieser sozusagen vorgestarteten Jobs, so baut sich zügig eine FTP-Sitzung auf. Ein FTP-Client, für den sich kein vorgestarteter Server-Job findet, muß dann zuerst den Start seines Server-Jobs beantragen, ein etwas länger andauernder Vorgang. Der Parameter Zeitüberschreitung bei Inaktivität bestimmt dann, wann eine FTP-Sitzung wieder freigegeben wird. Ist eine FTP-Sitzung 300 Se-

kunden nicht aktiv, so wird der FTP-Server wieder freigegeben und ein anderer Client kann sich dieses Server-Jobs bedienen. 300 Sekunden (5 Minuten) ist der Standardwert.

Soll FTP händisch gestartet werden, so erreichen Sie das mit dem Befehl STRTCPSVR *FTP. Die Beendung der FTP-Server erfolgt mit dem Befehl ENDTCPSVR *FTP.

Ist FTP gestartet, so sollten Sie im Subsystem QSYSWRK mehrere Jobs mit dem Namen QTFTPx sehen (x steht für eine von OS/400 generierte Zahl).



Die vorgestarteten FTP-Server-Jobs

Überprüfen Sie auch die Funktion der Ports 20 und 21, indem Sie den Befehl NETSTAT *CNN eingeben. In der Spalte lokale Ports finden Sie die angegebenen Port-Nummern, wenn Sie die F14-Taste betätigt haben. Beide Ports sollten den Status „Empfangsbereit“ aufweisen.

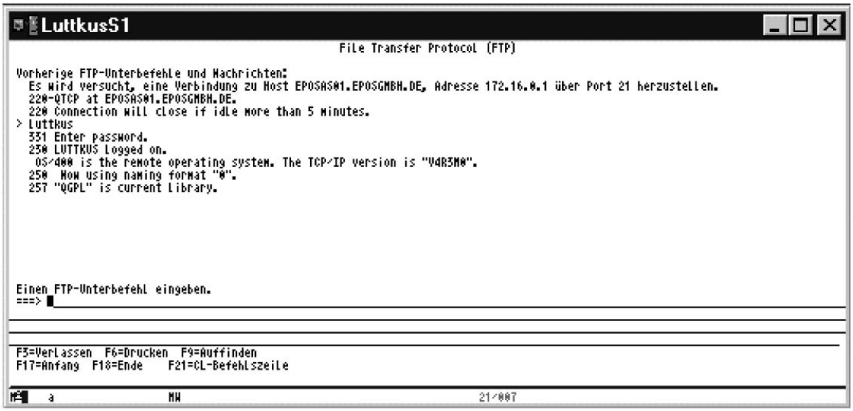
5.4.2.2 FTP-Client starten

In diesem Kapitel werde ich davon ausgehen, das Daten zwischen zwei AS/400-Systemen transferiert werden sollen. Die erste AS/400 ist über die IP-Adresse 172.16.0.1 zu erreichen; dieser Adresse ist der Host-Name EPOSAS01.EPOS.GMBH.DE zugeordnet worden. Das zweite System ist mit Hilfe der IP-Adresse 172.16.0.3 zu erreichen und trägt den Host-Namen EPOSAS03.EPOS.GMBH.DE. Ich habe mich am Host EPOSAS03.EPOS.GMBH.DE angemeldet.

Auf einer beliebigen Befehlszeile gebe ich folgenden Befehl ein: FTP EPOSAS01.EPOS.GMBH.DE

Sie erfahren aus diesem Bildschirm, daß die Datenübertragung über den Port 21 realisiert wird, daß diese Sitzung nach fünf Minuten wieder aufgeben wird, wenn Sie in dieser Zeitspanne keine Befehle eingeben und daß Sie aufgefordert werden eine korrekte Anmeldung zu vollziehen.

Nach kurzer Zeit baut sich der gezeigte Bildschirm auf .



Eine FTP-Verbindung ist aufgebaut

Haben Sie sich auf der entfernten Seite korrekt angemeldet, so besteht jetzt eine FTP-Verbindung zwischen EPOSAS03 und EPOSAS01.

Mit Hilfe der Befehlszeile übermitteln wir dann dem FTP-Server-Job auf dem Host EPOSAS01.EPOS.GMBH.DE, welche Objekte wir zu transferieren beabsichtigen. Im folgenden habe ich Ihnen einige der wichtigsten Befehle aus der FTP-Dokumentation herausgezogen:

Befehl	Bedeutung
\	Verzeichniswechsel im entfernten System
CD	Dito
CDUp	Verzeichniswechsel aufwärts
?	Hilfe anfordern
Help	Dito
Ascii	Datenformat anwählen
Binary	Dito
DELete	Objekt löschen
Mdelete	mehrere Objekte löschen
REName	Objekt neu benamen
Dir	Verzeichnisinhalt anzeigen
Mkdir	Neues Verzeichnis erstellen
RMDir	Verzeichnis entfernen

Get	Objekt holen
Mget	mehrere Objekte holen
Open	Sitzung anfordern
Put	Objekt bringen
Mput	mehrere Objekte bringen
PWd	aktuelles Verzeichnis anzeigen
User	Benutzerprofileingabe anfordern
Password	Kennworteingabe anfordern
QUIt	FTP-Sitzung beenden

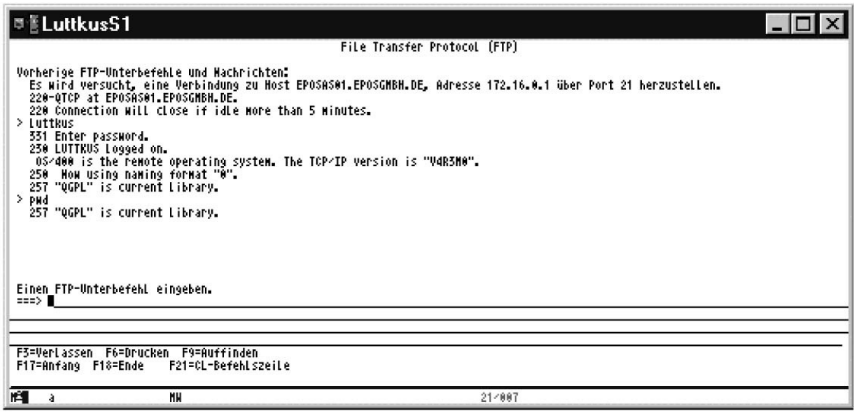
Wichtige FTP-Befehle

Soweit so gut. Was wissen wir bis jetzt? Wir wissen, daß uns der FTP-Client eine interaktive Oberfläche zur Verfügung stellt, mit der wir Daten von einem FTP-Server abholen und zu einem FTP-Server senden können.

5.4.2.3 Einen einfachen Transfer durchführen

Um Daten zu einem Server zu senden, wird der FTP-Befehl PUT verwendet – mehrere Dateien übertragen Sie mit dem Befehl MPUT (Multiples Senden). Um Daten von einem Server zu holen, wird der FTP-Befehl GET verwendet – mehrere Dateien holen Sie mit dem Befehl MGET (Multiples Holen). Wir werden jetzt versuchen, Daten aus der Bibliothek EPSSVFIL des Hosts EPOSAS01.EPOS.GMBH.DE zu holen (herunterzuladen).

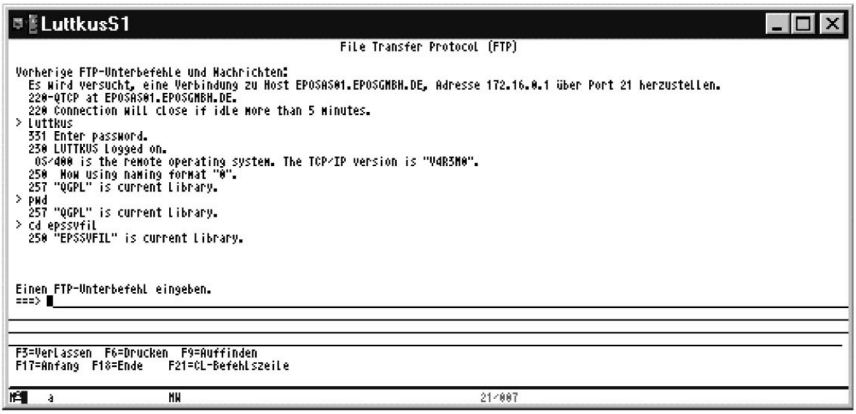
Aber Halt! Wir haben zwar eine Verbindung zum FTP-Server des Systems EPOSAS01.EPOS.GMBH.DE aufgebaut, aber wo – in welcher Bibliothek dieser AS/400 – befinden wir uns jetzt. Um diese Frage beantworten zu können, geben Sie einfach den Befehl PWD (Print Work Directory) ein.



FTP-Befehl: PWD – Print Work Directory

Ist in dem Benutzerprofil, das die Verbindung zum FTP-Server steuert, eine aktuelle Bibliothek definiert worden, so erscheint jetzt der Name der aktuellen Bibliothek im Anzeigebildschirm des FTPs. Ist im Benutzerprofil jedoch keine aktuelle Bibliothek bezeichnet worden, so wird QGPL als aktuelle Bibliothek ausgegeben.

Da in meinem Benutzerprofil keine aktuelle Bibliothek bestimmt wurde, besteht jetzt eine Verbindung zur Bibliothek QGPL des entfernten Systems. Ich verwende den Befehl CD (Change Directory – Verzeichnis wechseln), um jetzt in die Bibliothek EPSSVFIL zu wechseln, und gebe folgenden Befehl ein: CD EPSSVFIL



Mit CD in die Bibliothek EPSSVFIL wechseln

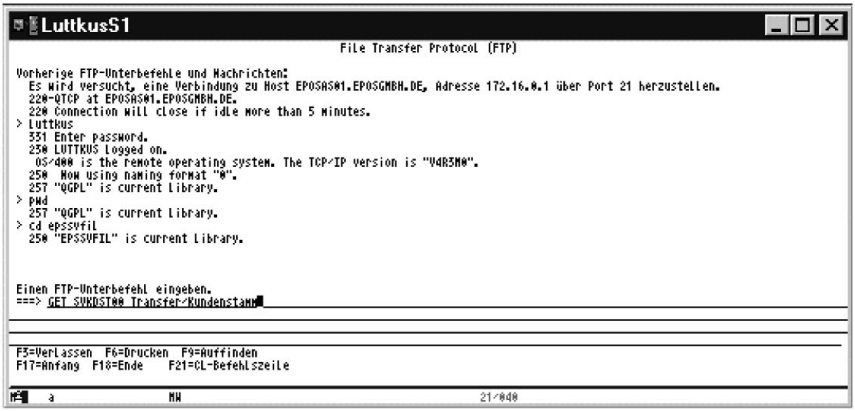
Existiert diese Bibliothek auf dem entfernten System und besitze ich Zugriffsrechte für diese Bibliothek, so wird die Meldung im FTP-Bildschirm ausgegeben, daß ab jetzt eine Verbindung zu dieser Bibliothek besteht.

Ich möchte nun Daten aus der Datei SVKDST00 (Kundenstammdaten) herunterladen. Diesen Vorgang realisiere ich mit dem FTP-Befehl GET. Das allgemeine Format dieses Befehls sieht wie folgt aus:

Get entfernte datei [lokale Datei] [(Replace]

- **Entfernte Datei:** Die Datei, die heruntergeladen werden soll. Die Angabe des gesammten Zugriffspfads ist möglich.
- **Lokale Datei:** Falls die Datei auf dem lokalen System noch nicht vorhanden ist, kann Sie unter einem anderen Namen erstellt werden. Ist die Datei lokal nicht vorhanden und wird dieser zweite Parameter nicht genutzt, dann wird die Datei lokal unter dem gleichen Namen angelegt wie auf dem entfernten System.
- **Replace:** Ist die Datei bereits lokal vorhanden und befinden sich in ihr Daten, so werden diese ersetzt, sofern dieser Parameter gesetzt wurde.

Ich gebe also folgende Befehlsfolge auf der Befehlszeile des FTP-Clients ein:



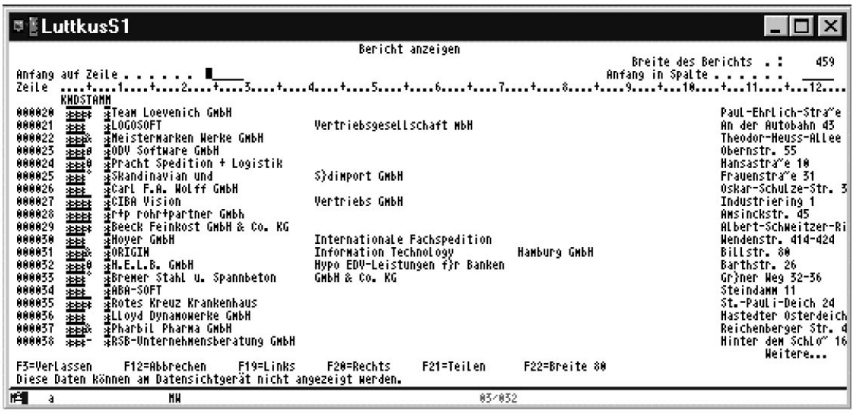
GET SVKDST00 TRANSFER/KNDSTAMM

Der Transfer ist beendet

Nach Bestätigung der Eingabe mit Datenfreigabe wird der Befehl ausgeführt. Ist alles korrekt verlaufen, stehen jetzt die Daten der entfernten Datei SVKDST00 auf dem lokalen Host EPOSAS03.EPOS.GMBH.DE in der Bibliothek TRANSFER in der Datei KNDSTAMM zur Verfügung.

Sehen wir uns jetzt einmal an, wie unsere Daten auf dem lokalen System EPOSAS03.EPOSGMBH.DE aussehen. Die Datei auf dem Host EPOSAS01 war eine ganz normale physische Datei, deren Felder extern beschrieben worden waren. Ich will damit sagen, daß die Feldbeschreibung für die Datei SVKDST00 Bestandteil der Objektbeschreibung der Datei ist.

Ich werde jetzt einfach den Befehl RUNQRY ausführen, um den Inhalt der Datei KNDSTAMM auf dem System EPOSAS03 anzuzeigen.



Anzeige der Daten in KNDSTAMM

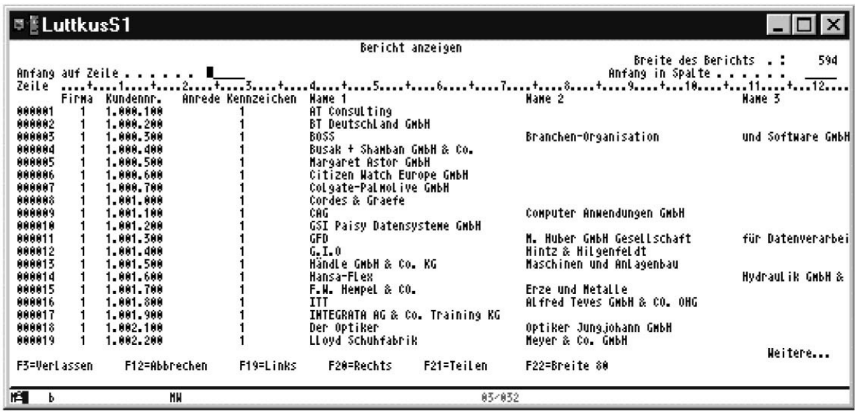
Zwei Dinge fallen sofort auf:

1. Ein Datensatz besteht nur noch aus einem einzigen Feld. D. h., daß die Feldbeschreibungen beim Transfer nicht übertragen wurden.

2. Am Anfang jedes Datensatzes befinden sich eigentlich drei numerische, gepackte Felder. Diese sind beim Transfer ebenfalls nicht korrekt umgesetzt worden.

Was können wir dagegen unternehmen? Der Trick liegt darin, daß wir die Zieldatei als Objekt erstellen.

Aber Vorsicht! Erstellen Sie die Datei mit dem Befehl CRTPF (Create Physical File – Physische Datei erstellen) oder mit CRTDUPOBJ (Create Duplicate Object – Objekt duplizieren), so wird automatisch eine leere Teildatei angelegt. Diese verhindert den Transfer! Entfernen Sie also die leere Teildatei mit dem Befehl RMVM (Remove Member – Teildatei entfernen) und führen Sie dann den Transfer erneut durch.



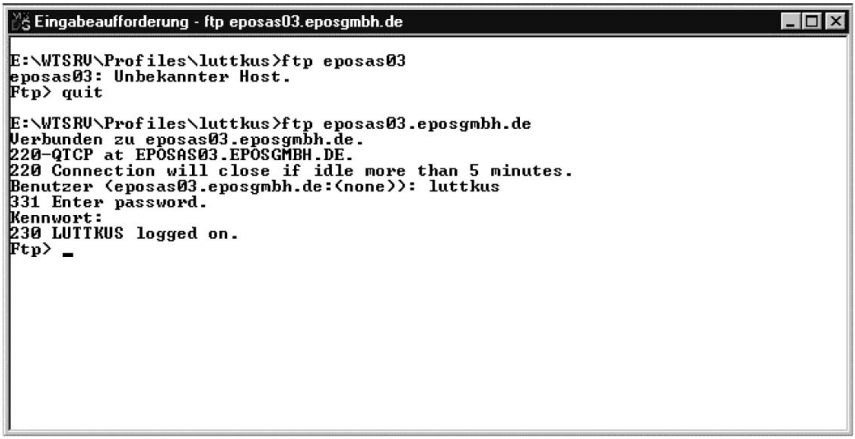
Inhalt der Datei KNDSTAMM – in erstellte Zieldatei

Sie sehen, daß beide o. a. Probleme in einem Arbeitsgang behoben wurden. Wir sehen anhand der Überschriften, daß externe Feldbeschreibungen angelegt sind und die gepackten numerischen Felder feldgerecht übertragen wurden.

5.4.2.4 FTP auf dem Windows PC

Haben Sie auf Ihrem Windows PC – und damit meine ich einen PC unter Windows for Workgroups, Windows 95/98 sowie Windows NT – TCP/IP als Transportprotokoll installiert und konfiguriert, so stehen Ihnen auch hier die gängigen TCP/IP-Dienste zur Verfügung. Um den Windows-FTP-Client zu starten, gehen Sie einfach in die DOS-Box Ihres Windows PCs und rufen dort den FTP-Client auf. Der Aufruf hat folgendes allgemeines Format:

FTP <Adresse bzw. Host-Name des FTP-Servers>



Der Verbindungsdialog

Da ich auf der AS/400 den FTP-Server konfiguriert und gestartet habe und diese AS/400 via TCP/IP erreichbar ist, stelle ich die Verbindung mit folgender Syntax her:

FTP 172.16.0.3 bzw. FTP eposas03.eposgmbh.de

In der ersten Variante dieser Adresse benutze ich die IP-Adresse, in der zweiten den Host-Namen, der entweder in der Host-Tabelle des Clients hinterlegt wurde oder in einem Domain Name Server (DNS). Sollte die Verbindung zustande gekommen sein, so werden Sie aufgefordert, sich an der AS/400 anzumelden und Sie sehen den folgenden Dialog:

Zeilen-Nr.	
10	D:\WTSRV>ftp eposas03.eposgmbh.de
20	Verbunden zu EPOSAS03.EPOSGMBH.DE.
30	220-QTCP at EPOSAS03.EPOSGMBH.DE.
40	220 Connection will close if idle more than 5 minutes.
50	Benutzer (EPOSAS03.EPOSGMBH.DE:(none)): luttkus
60	331 Enter password.
70	Kennwort:
80	230 LUTTKUS logged on.
90	Ftp>

Die Zeilennummern habe ich eingefügt, sie dienen der besseren Übersicht.

- In Zeile 10 sehen Sie den DOS-Prompt mit dem Aufruf des Befehls FTP.
- Zeile 20 ist eine Statusmeldung des FTP-Clients und spricht für sich selbst.
- Zeile 30 ist eine Statusmeldung des FTP-Servers und besagt, daß mit Hilfe des Benutzers QTCP die Verbindung hergestellt wurde.
- Zeile 40 besagt, daß die Verbindung wieder aufgegeben wird, sofern der Benutzer innerhalb von 5 Minuten keinen FTP-Befehl eingibt. Sollte dies einmal der Fall sein, läßt sich die FTP-Sitzung mit dem Befehl OPEN wieder aufnehmen.
- Zeile 50 fordert dann die Eingabe eines aktiven AS/400-Benutzerprofils an.
- Zeile 60 fordert die Eingabe des entsprechenden Kennworts an.
- Zeile 70 stellt das Eingabefeld zur Verfügung. Eingaben sind nicht sichtbar.
- Zeile 80 ist eine Statusmeldung des FTP-Server-Jobs der AS/400 und besagt, daß die Anmeldung korrekt war.
- Zeile 90 ist der Eingabe-Prompt für FTP-Befehle.

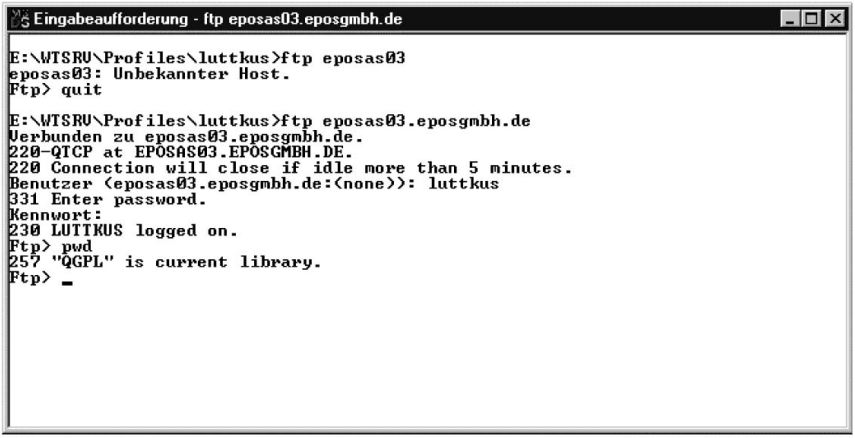
An dieser Stelle können wir jetzt FTP-Befehle eingeben. Bevor wir jedoch damit beginnen, einen Transfer durchzuführen, sollten wir uns einige Gedanken bezüglich der Fähigkeiten des FTPs machen. Welche Daten lassen sich mit Hilfe von FTP übertragen? Die Anwort ist eigentlich simpel: alles was auf der AS/400 in irgendeiner Form Objektstatus hat, kann mittels FTP übertragen werden. Also nicht nur Datenbankinhalte, sondern rein theoretisch auch Programme, Bildschirmbeschreibungen usw., usf.

Wichtig für uns ist jedoch der Standort der Daten. Bedenken Sie, daß wir es auf der AS/400 mit zwei unterschiedlichen Datenhaltungssystemen zu tun haben. Einmal mit dem Integrated File System, in dem Daten in hierarchischer Ordnung abgelegt werden, und zum anderen mit dem Bibliothekssystem, das keine hierarchische Ordnung kennt.

5.4.2.5 Das AS/400-Bibliothekssystem

Haben wir eine FTP-Sitzung aufgebaut, so greifen wir über das AS/400-Bibliothekssystem auf unsere Daten zu. Das bedeutet für uns, daß wir mittels FTP nur auf die Datenbankobjekte der AS/400 zugreifen können. Das ist für uns ebenfalls Stand der Dinge. Und auf welche Datenbankdateien können wir jetzt zugreifen? Auch hier wieder eine einfache Antwort. Auf alle Datenbankdateien, für die wir die entsprechenden Zugriffsrechte besitzen – da wir auf solche Objekte mit Hilfe der Pfadangabe Bibliothek/Datenbank-Objekt zugreifen. Dieses Format wird von FTP als das Namensfomat 0 (NAMEFMT 0) bezeichnet.

Eine weitere, uns interessierende Frage ist sicherlich, in welcher Bibliothek wir nun stehen. Diese Frage läßt sich unter Verweis auf das Benutzerprofil beantworten, mit dem wir die FTP-Sitzung aufgebaut haben. Ist über das verwendete Benutzerprofil keine aktuelle Bibliothek bezeichnet worden, so befinden wir uns nach Aufbau der FTP-Sitzung in der Bibliothek QGPL. Wird mittels des Benutzerprofils eine Bibliothek bezeichnet, so befinden wir uns nach FTP-Sitzungsaufbau in der bezeichneten Bibliothek. Im Benutzerprofil Luttkus ist jedoch keine aktuelle Bibliothek bezeichnet, folglich befinden wir ins in der Bibliothek QGPL.

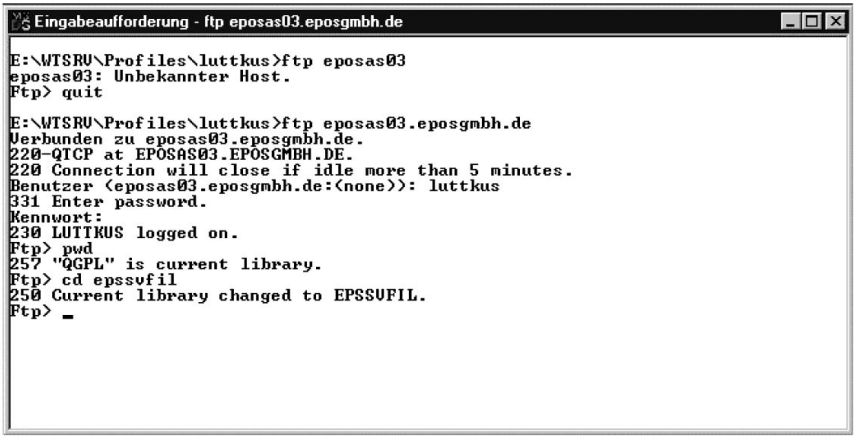


PWD – Print Work Directory

Mit dem Befehl PWD (Print Work Directory) können wir uns unseren aktuelle Standort anzeigen lassen.

Ftp> pwd
257 „QGPL“ is current library.
Ftp>

Um die Bibliothek zu wechseln, nutzen wir den Befehl CD (Change Directory). Dieser Befehl wechselt auf dem Server-System die aktuelle Bibliothek.



In die Bibliothek EPSSVFIL wechseln

Ich werde jetzt in die Bibliothek EPSSVFIL wechseln und gebe folgenden Befehl am FTP-Prompt ein:

Ftp> cd epssvfil
250 Current library changed to EPSSVFIL.
Ftp>

Mit Hilfe von GET-Befehlen können nun Daten auf den PC-Client heruntergeladen werden. Mit PUT-Befehlen übertragen wir Daten vom Client auf die AS/400.

5.4.2.6 Das Integrated File System

Beabsichtigen wir jedoch, nicht nur Daten aus dem Datenbankbereich der AS/400 zu übertragen, so kommen wir mit dem bisher Gesehenen nicht weiter. Lassen Sie uns ein einfaches Beispiel entwickeln. Wir beabsichtigen ein Dokument aus dem Verzeichnis Home, das auf dem Host EPOSAS03.EPOSGMBH.DE eingerichtet wurde, an einen PC zu übertragen. Hierbei handelt es sich um ein Dokument mit dem Namen ADRESSEN.TXT.

Wenn wir jetzt einfach mit dem Befehl CD in den Ordner PCQTEMP wechseln, so erhalten wir eine Fehlermeldung.

```
Ftp> cd pcqtemp
550-Specified library does not exist or cannot be accessed.
550 Current library not changed.
Ftp>
```

Was ist der Grund für diesen Fehler? Die AS/400-Verzeichnisse sind nicht Bestandteil des Bibliothekssystems, sondern als hierarchischer Lagerort direkter Bestandteil des Integrated File System (IFS) und können damit auch nur über das IFS angesprochen werden. Beabsichtigen wir, unsere Daten über das IFS anzusprechen, so muß der FTP-Server der AS/400 auf das Namensformat 1 umgestellt werden. Jetzt greifen wir auf unsere Daten mittels der folgenden Pfadangabe zu:

/Verzeichnis/.../.../Objekt.Extension

Auf unser Beispiel bezogen, wäre die korrekte Pfadangabe:

/HOME/ADRESSEN.TXT

Also modifizieren wir die vorhin verwendete CD-Anweisung und geben folgendes ein:

```
Ftp> cd /home
250-NAMEFMT set to 1.
250 Current directory changed to /home.
Ftp>
```

Sie sehen, daß die modifizierte Eingabe des Befehls CD das Namensformat auf den Wert 1 gesetzt hat. Alle objektbezogenen Zugriffe werden jetzt IFS-bezogen dargestellt. Ich gebe nun einfach den Befehl PWD ein.

```
Ftp> pwd
257 Current directory is „/home“.
Ftp>
```

Auch hier sehen Sie die entsprechende pfadbezogene Syntax.

Lassen Sie uns nun zur Tat schreiten und das Dokument ADRESSEN.TXT aus dem IFS-Pfad /home in das Verzeichnis D:\LUTTKUS meines PCs übertragen. Dazu benutzen wir den Befehl GET:

```
Ftp> get adressen.txt d:\luttkus
```

Befinden wir uns nicht in dem Verzeichnis, aus dem Daten transferiert werden, so kann das Quellobjekt auch mit seiner gesamten Pfadangabe angesprochen werden:

```
Ftp> get /home/adressen.txt d:\luttkus
```

Beabsichtigen wir nun, Daten (SVKDST00) aus einer Datenbankdatei (EPSSVFIL) zu übertragen so muß die Syntax folgendermaßen aussehen:

```
Ftp> get /qsys.lib/epssvfil.lib/svkdst00.file
```

200 PORT subcommand request successful.

150 Retrieving member SVKDST00 in file SVKDST00 in library EPSSVFIL.

250 File transfer completed successfully.
1658652 Bytes empfangen in 2,39 Sekunden (693,13 KB/s)

Ftp>

Beachten Sie, daß die Objektarten der AS/400 als Namenserweiterungen den Objektnamen hinzugefügt werden müssen!

Erfolg!
Die Daten wurden übertragen. Jedoch: Sie werden sagen, diese Pfadangabe, die relativ lang und anfällig für Tippfehler ist, könnte ich auch vermeiden, wenn ich das bibliotheksbezogene Namensformat wieder zurückstellen könnte. Nichts einfacher als das. Hierzu verwenden wir einen Befehl namens QUOTE, der dazu dient, sogenannte Subcommands an den FTP-Server der AS/400 zu übertragen.

Ftp> quote site namefmt 0
250 Now using naming format „0“.
Ftp>

Der gleiche Transfer sieht im Namensformat 0 dann so aus:

Ftp> get svkdst00
200 PORT subcommand request successful.
150 Retrieving member SVKDST00 in file SVKDST00 in library EPSSVFIL.
250 File transfer completed successfully.
1658652 Bytes empfangen in 2,36 Sekunden (701,63 KB/s)
Ftp>

Wollen Sie das Namensformat des Zugriffs auf bestimmte Daten ändern, so geben Sie folgende FTP-Befehle ein:

Ftp> quote site namefmt 0
Bibliotheksbezogener Zugriffspfad ist eingestellt. Achtung! Nur Objekte, die mit Hilfe der Bibliothek QSYS verwaltet werden, können übertragen werden.

Ftp> quote site namefmt 1
IFS-Verzeichnis-bezogener Zugriffspfad ist eingestellt. Jedes Objekt des gesamten Integrated File System kann übertragen werden.

5.4.2.7 FTP im Batch

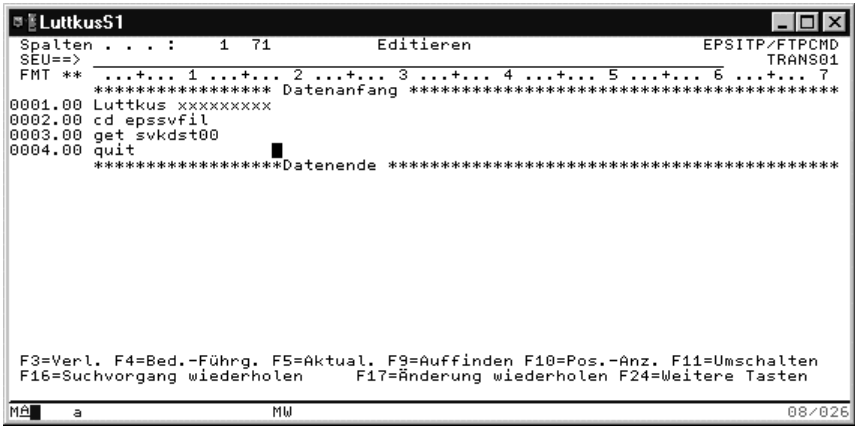
Sowohl der FTP-Client der AS/400 als auch der FTP-Client des Windows können im Batch-Betrieb ausgeführt werden. In den folgenden Abschnitten werde ich das Vorgehen für beide Clients beschreiben.

5.4.2.7.1 AS/400-FTP im Batch

Der FTP-Client der AS/400 ist eigentlich eine rein interaktive Komponente, jedoch läßt sich die Interaktivität einfach beseitigen. Der Bildschirm wird vom FTP-Client als sogenannte Standard-Ein- und -Ausgabeeinheit angesehen. Die Standardeingabeeinheit wird systemtechnisch mit dem Namen INPUT angesprochen, die Standardausgabeeinheit mit dem Namen OUTPUT. Wir könnten einfach formulieren: Die Befehlseingabe wird eigentlich aus einer Datei namens INPUT erwartet. Ist diese Datei physisch nicht vorhanden, so schaltet der FTP-Client einfach auf Bildschirmeingabe um. Das gleiche gilt für protokollarische Ausgaben. Es wird davon ausgegangen, daß eine Datei mit dem Namen OUTPUT auf dem System ist. Falls nicht, wird die Ausgabe auf den Bildschirm gelenkt.

In diesen Aussagen steckt auch schon der Ansatz für die Vorgehensweise beim Batch-gesteuerten Dateitransfer.

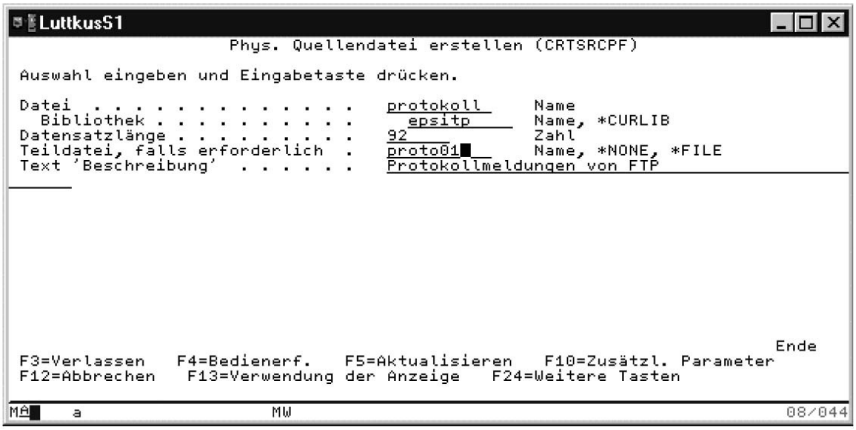
In einem ersten Arbeitsschritt erzeuge ich eine Quelldatei mit dem Namen FTPCMD. In diese Datei nehme ich eine Teildatei mit dem Namen TRANS01 auf. Diese Teildatei enthält die Befehle, die für die Ausführung des Transfers notwendig sind.



FTP-Befehle in der Datei FTPCMD MBR(TRANS01)

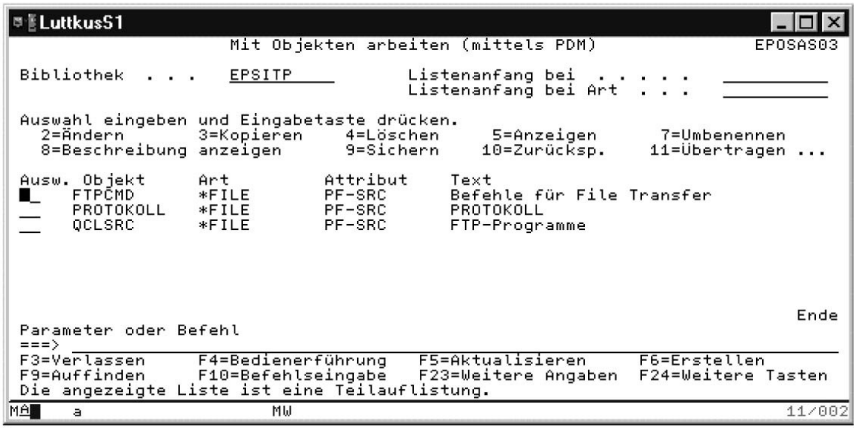
Zeilennummer	Beschreibung
1	Übergabe der Berechtigungsdaten. Achtung! Bei einem Transfer von bzw. zu einem anderen System AS/400 müssen Sie hier ein valides Benutzerprofil inklusive Kennwort angeben. Seien Sie sich dieses Sicherheitsaspektes bewußt und schützen Sie diese Datei auf der Objektebene!
2	In die Bibliothek wechseln, in der die zu übertragende Datei steht.
3	Datei übertragen. Hier wird eine Datei von einem entfernten System heruntergeladen.
4	Die FTP-Verbindung beenden.

In einem zweiten Arbeitsschritt wird jetzt die Ausgabedatei PROTOKOLL mit einer Teildatei PROTO01 erstellt.



CRTSRCPF – Create Source Physical File

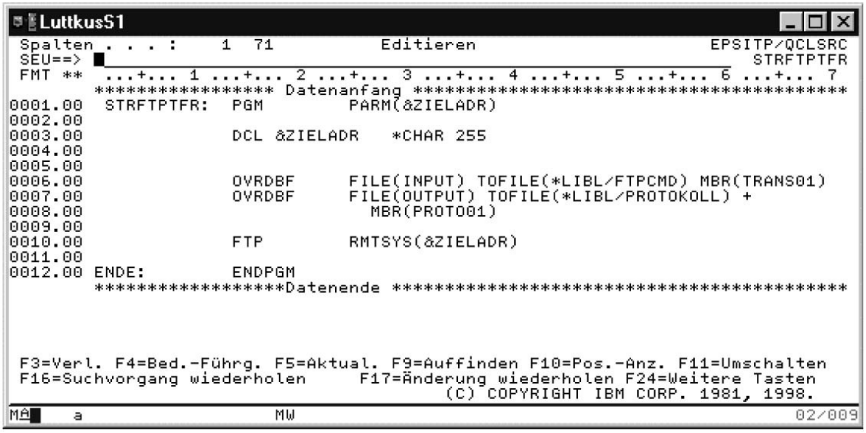
In einem dritten Schritt erstelle ich auch eine Quelldatei für das CL-Programm, das den Transfer letztendlich ausführen soll .



Die Quelldatei QCLSRC ist erstellt

Im vierten Arbeitsschritt wird das CL-Programm erstellt.

Dieses Programm heißt STRFTPTFR (Start FTP-Transfer). Die Quelle sehen Sie in folgendem Bild.



Das CL-Programm STRFTPTFR

Zeilennummer	Beschreibung
1	Übergabe der Zieladresse für den Transfer als Parameter.
6	Den Namen der Datei INPUT mit dem Namen der Befehlseingabedatei FTPCMD/TRANS01 überschreiben. Dadurch wird die Befehlseingabedatei als Datei INPUT angesprochen.

7	Den Namen der Datei OUTPUT mit dem Namen der Befehlseingabedatei PROTOKOLL/PROTO01 überschreiben. Dadurch wird die Befehlseingabedatei als Datei OUTPUT angesprochen.
10	Den Transfer durchführen.

Jetzt wird das Programm STRFTPTFR mit dem Befehl CRTCLPGM umgewandelt und kann dann ausgeführt werden.

CALL PGM(STRFTPTFR) PARM(‚172.16.0.1‘)

Als Parameter wird die Adresse des TCP/IP-Hosts angegeben, von dem die Datei zu transferieren ist.

Folgende Meldungen sind dann der Datei PROTOKOLL zu entnehmen:

Aufnahme der Verbindung mit dem entfernten System.

Ausgabe wurde in eine Datei umgeleitet.
Eingabe aus angegebener Überschreibungsdatei wurde gelesen.
Versuch, eine Verbindung zum fernen Host 172.16.0.1 über Port 21 herzustellen.

220-QTCP at EPOSAS02.EPOSGMBH.COM.
220 Connection will close if idle more than 5 minutes.

Anmeldung des Benutzers, der für den Transfer verantwortlich ist.
Anmelde-ID (luttkus) eingeben:
331 Enter password.
230 LUTTKUS logged on.

OS/400 is the remote operating system. The TCP/IP version is „V4R3M0“.
250 Now using naming format „0“.
257 „QGPL“ is current library.
Einen FTP-Unterbefehl eingeben.

Wechseln in die Bibliothek, aus der die Daten entnommen werden sollen.
> cd epssvfil
250 Current library changed to EPSSVFIL.
Einen FTP-Unterbefehl eingeben.

Die Daten herunterladen.
> get svkdst00
250 Now using naming format „0“.
257 „EPSSVFIL“ is current library.
227 Entering Passive Mode (172,16,0,1,4,1).
150 Retrieving member SVKDST00 in file SVKDST00 in library EPSSVFIL.
250 File transfer completed successfully.
969449 Byte in 31.415 Sekunden übertragen. Übertragungsgeschwindigkeit 30.859 KB/s.

Die FTP-Verbindung beenden.
Einen FTP-Unterbefehl eingeben.
> quit
221 QUIT subcommand received.

5.4.2.7.2 Windows-FTP im Batch

Auch der Windows FTP-Client kennt den Stapelmodus. Im Prinzip wird hier analog zum AS/400-FTP verfahren. Die einzugebenden FTP-Befehle werden aus einer Eingabedatei entnommen, die der Anwender zu erstellen hat.

Um den Vorgang zu verstehen, sehen wir uns zuerst die Parameter des Windows-Befehls FTP an:

FTP [-v] [-d] [-i] [-n] [-g] [-s:Dateiname] [-a] [-w:Puffergröße] [Host]

-v Unterdrückt die Anzeige von Rückmeldungen des Remote-Servers.

-n Unterdrückt die automatische Anmeldung beim Verbindungsaufbau.

-i Schaltet interaktive Eingabeaufforderungen beim Transfer von mehreren Dateien ab.

-d Aktiviert Debug-Modus.

-g Deaktiviert Globbing (siehe Befehl Ftp: glob).

-s: Dateiname
Gibt eine Textdatei mit FTP-Befehlen an; die Befehle werden automatisch ausgeführt, wenn FTP gestartet wird.

-a Verwendet beim Binden von Datenverbindungen eine beliebige lokale Schnittstelle.

-w: Puffergröße, ändert die Standardgröße des Übertragungspuffers in 4096.

Host Gibt den Host-Namen oder die IP-Adresse des Remote-Hosts an, zu dem eine Verbindung hergestellt werden soll.

Ich habe den Parameter, der für unser Vorhaben maßgeblich ist, grau hinterlegt.

Verwenden wir den Parameter -s, so werden die FTP-Befehle mit Hilfe einer Input-Datei an den FTP-Client übergeben. Daraus ergibt sich folgende Vorgehensweise.

1.) Ich erstelle auf meiner Windows NT Workstation eine Textdatei mit dem Namen FTPCMD.TXT. Dazu nutze ich den Befehl EDIT der DOS-Box meiner Workstation.

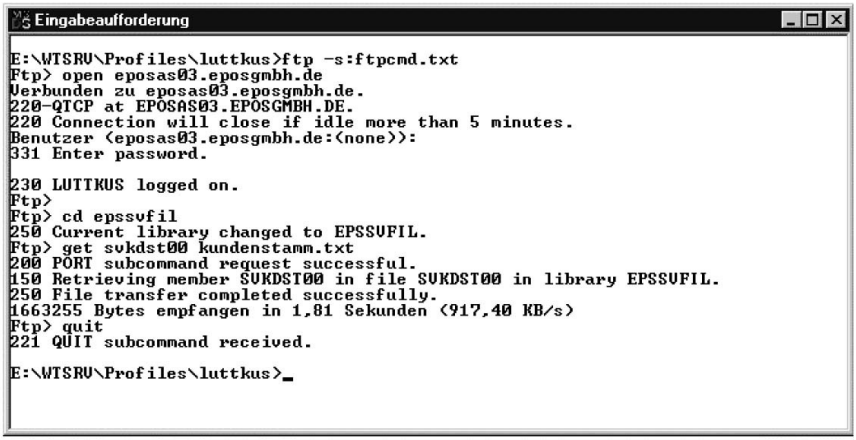
Die Datei FTPCMD.TXT

Achtung: Beachten Sie die Eingabe des Benutzerprofils und des Kennworts. Die hier gezeigte Syntax ist für den AS/400-FTP-Server peinlich genau einzuhalten!

2.) Jetzt rufe ich den Windows FTP-Client mit folgender Syntax auf:

FTP–S:FTPCMD.TXT

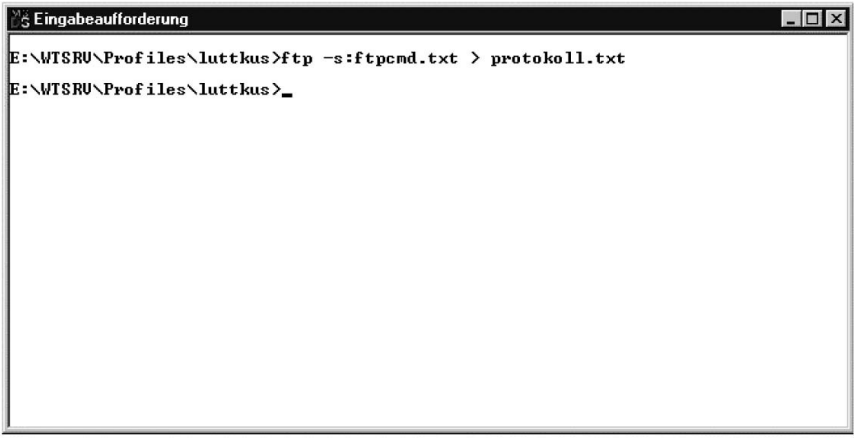
Bei der Befehlsausführung, werden alle Ausführungsschritte auf dem Bildschirm dargestellt.



Textausgabe des Batch-gesteuerten Windows FTPs

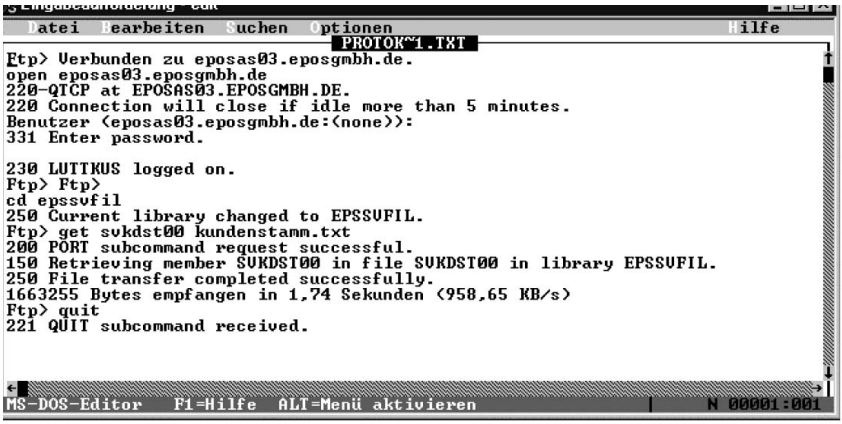
Soll diese Textausgabe unterdrückt werden, so kann die Bildschirmausgabe mit Hilfe einer DOS-Pipe in eine Datei umgelenkt werden. Dazu nutze ich folgende Syntax:

FTP –S:FTPCMD.TXT > PROTOKOLL.TXT



Unterdrückte Bildschirmausgabe

Um eine Aussage darüber treffen zu können, wie der Transfer ausgegangen ist, öffne ich jetzt mit Hilfe des Befehls EDIT die Datei PROTOKOLL.TXT.



Inhalt der Datei PROTOKOLL.TXT

5.4.2.8 FTP zum Windows PC

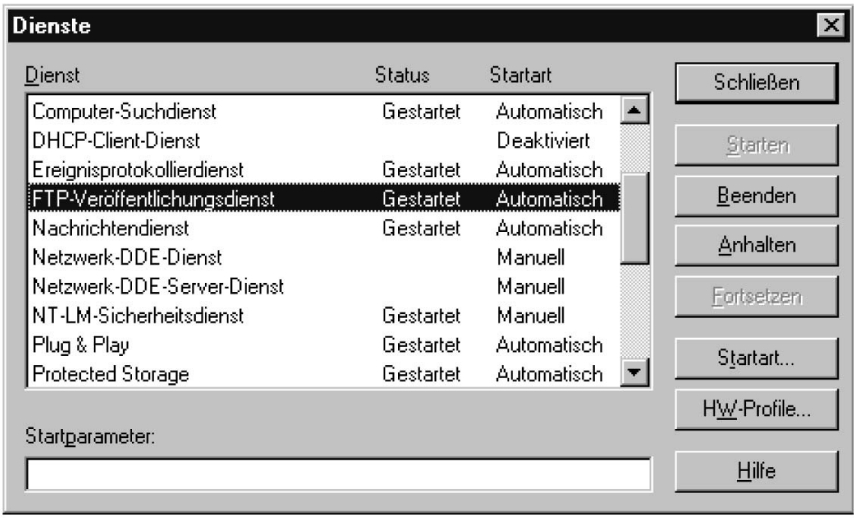
Nachdem wir jetzt Daten quasi automatisch von einer AS/400 und einem Windows PC herunter- bzw. heraufladen können, sollte es eigentlich möglich sein, diesen Prozeß auch von der AS/400 aus gegen einen PC zu richten. Wir wollen erreichen, daß die AS/400 einem PC-Client direkt Daten zusenden kann. Also nicht, daß der PC sich Daten von der AS/400 abholt, sondern daß die AS/400 aktiv Daten an einen PC sendet .

Dazu müssen wir auf einem Windows PC einen FTP-Server installieren. Besitzen Sie eine Windows NT Workstation, so sind Sie bereits im Besitz eines FTP-Servers. Dieser wird zwar nicht automatisch installiert, kann aber leicht nachinstalliert werden. Bestandteil der Windows NT Workstation ist ein sogenannter Peer Webserver und Bestandteil dieses Web-Servers ist wiederum ein FTP-Server.

Mittels des Windows NT-Dialogs „Netzwerkumgebung-Eigenschaften-Dienste-hinzufügen“ installieren Sie einfach den Microsoft Peer Webserver nach.

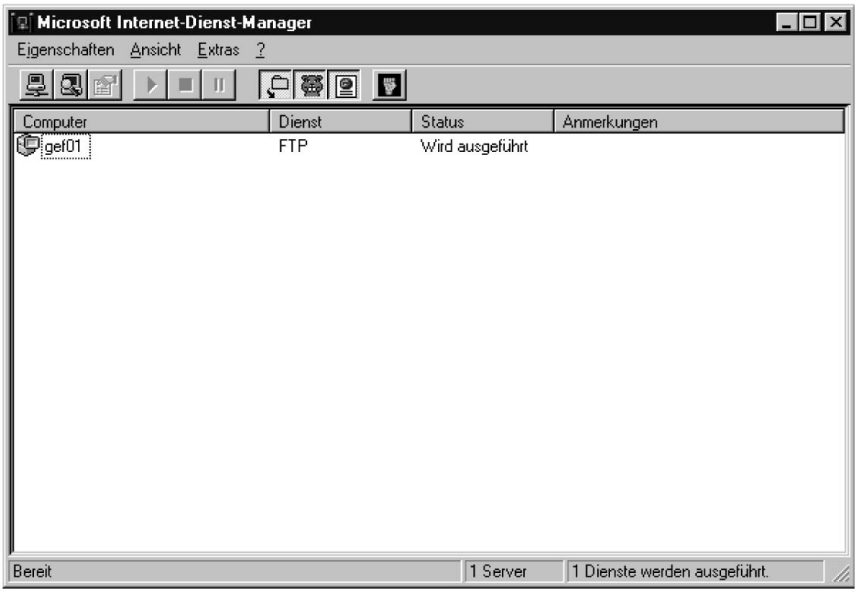
Der Microsoft Peer Webserver wurde installiert

Damit dieser Server in Betrieb genommen werden kann, muß der soeben installierte Dienst manuell gestartet werden. Soll jedoch der FTP-Server ständig in Betrieb sein, so sollten Sie die Startart dieses Dienstes von manuell auf automatisch ändern. Das erreichen Sie im Dialog „Systemsteuerung – Dienste“.



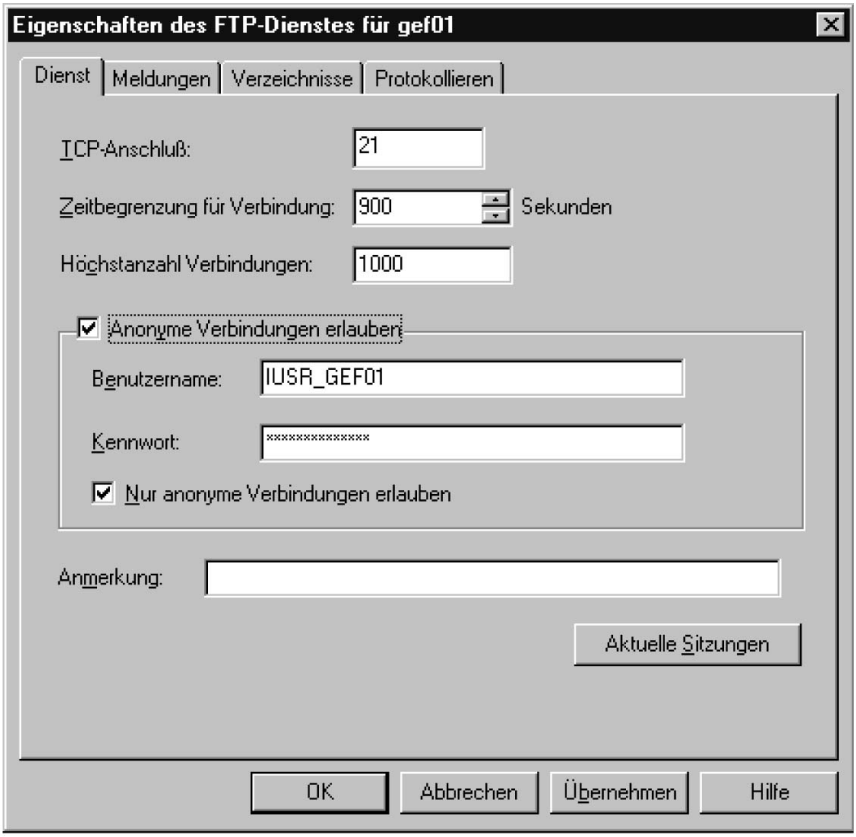
FTP automatisch starten

Bevor Sie jedoch den FTP-Server in Betrieb nehmen können, muß er zuerst einmal konfiguriert werden.



Der Internet-Dienst-Manager

Rufen Sie daher aus dem Dialog Start – Programme – Microsoft Peer Web Services – Internet-Dienst-Manager das Verwaltungsprogramm auf und konfigurieren Sie folgende Merkmale über den „Eigenschaften“-Dialog des angezeigten FTP-Dienstes:



Register „Dienst“

Register „Dienst“: Anonyme Verbindungen erlauben oder entziehen.

Gestatten Sie keine anonyme Verbindung, so richtet sich der Anmeldungsprozeß der AS/400 als FTP-Client gegen einen registrierten lokalen Benutzer der Workstation. Es wird bei der Installation des Peer Webservers ein lokales NT-Benutzerkonto erstellt. Der Name des Benutzers wird vom System generiert. Für diesen

Fall habe ich das Kennwort ftp vergeben. Diese Angaben sind wichtig! Der FTP-Client der AS/400 wird sich später mit diesem Berechtigungsdaten beim Windows NT FTP berechtigen lassen müssen. Beachten Sie, daß Windows NT bei der Schreibweise des Kennwortes Groß- und Kleinschreibung unterscheidet!

Register „Verzeichnisse“

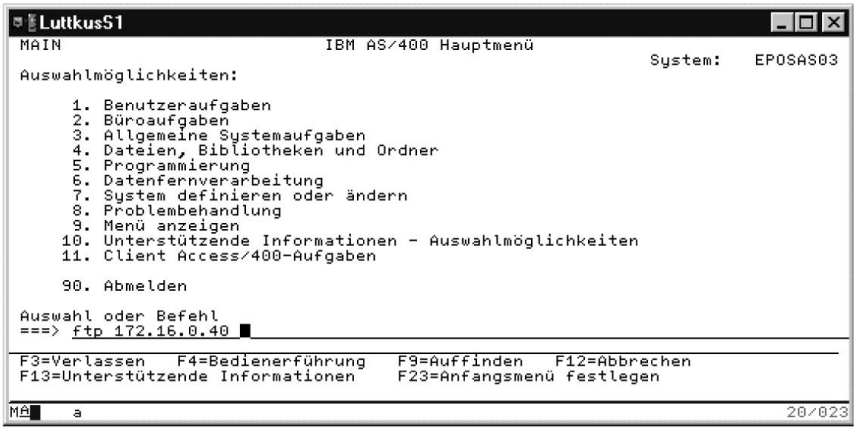
Register „Verzeichnisse“: Richten Sie hier das Verzeichnis ein, in das die Daten von der AS/400 heruntergeladen werden sollen. Ich habe es hier bei den Default-Einstellungen belassen.

Wichtig: Ändern Sie das Verzeichnisformat auf MS-DOS. Vergeben Sie sodann mit Hilfe des Dialogs „Eigenschaften bearbeiten“ Schreibrechte für das angezeigte Verzeichnis. Die AS/400 soll ja Daten auf den PC herunterladen, also benötigen Sie auch die entsprechenden Rechte.

Haben Sie alles erledigt, so sollten Sie kontrollieren, ob der Dienst korrekt arbeitet. Das erreichen Sie, indem Sie in das Windows NT-Ereignisprotokoll gehen. Läuft alles korrekt, so kann das Herunterladen von AS/400-Daten beginnen.

Wir werden zuerst einmal den Vorgang interaktiv testen:

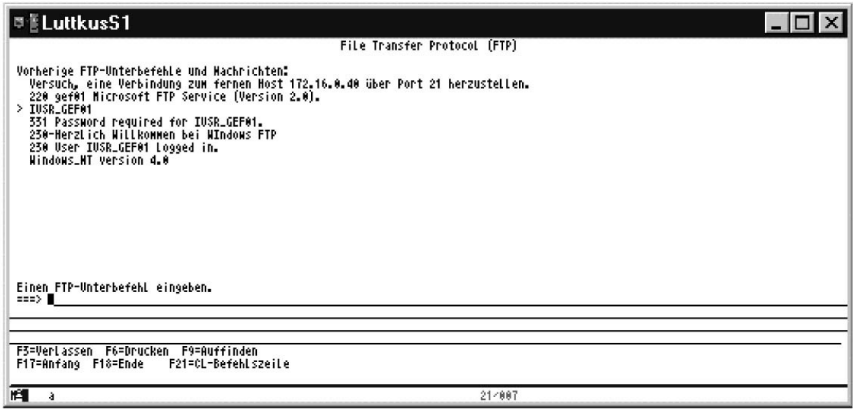
1. FTP auf der AS/400 aufrufen.



FTP aufrufen

Ich übergebe hier als Adresse die IP-Adresse des PCs, auf dem der FTP-Server-Dienst ausgeführt wird.

2. FTP-Berechtigungsdaten eingeben.



Die Anmeldung

Bei der Anmeldung habe ich das lokale Benutzerkonto IUSF_GEF01, das bei der Installation des FTP-Servers erzeugt wurde, verwendet.

3. Daten transferieren.

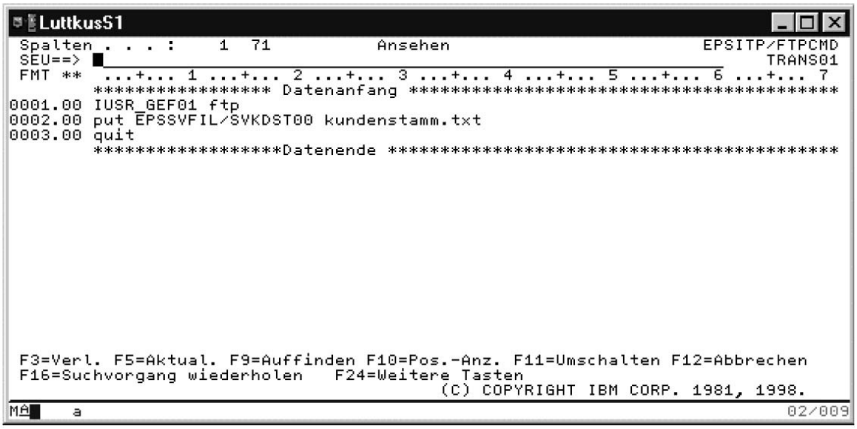
Daten senden

Mit Hilfe des FTP-Befehls PUT werden die Daten auf den PC transferiert.

Die Daten wurden gesendet

Danach wird mit QUIT die FTP-Verbindung beendet. Die Daten stehen zur weiteren Verarbeitung auf der Workstation zur Verfügung.

Soll der Transfer automatisiert werden, so greife ich auf meine vorhin erstellte Datei FTPCMD zurück, die dazu ein wenig verändert werden muß:



Die Datei FTPCMD MBR(TRANS01)

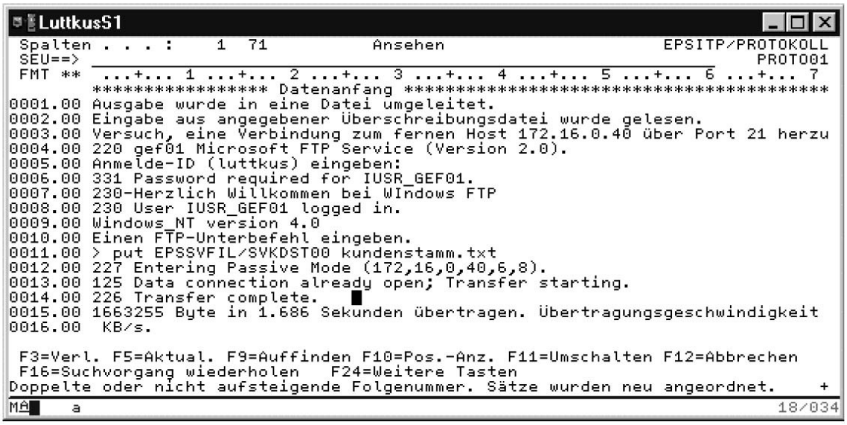
Wichtig ist die Zeile 1! Hier tragen Sie den Namen eines auf der NT Workstation registrierten Benutzers ein. Achtung! Windows NT unterscheidet keine Groß- und Kleinschreibung im Benutzernamen. Es wird jedoch die Schreibweise des Kennwortes peinlichst genau unterschieden.

Wichtig ist ebenfalls Zeile 2! Der Zugriffspfad zur AS/400-Datei muß in Großschreibung eingegeben werden, sonst wird die Datei nicht gefunden.

Ich rufe also unser Transferprogramm auf und gebe als Zieladresse den Windows NT PC an.

CALL PGM(STRFTPTFR) PARM(‚172.16.0.40‘)

Jetzt wird der Transfer ausgeführt. Um das Ergebnis des Transfers zu überprüfen, sehe ich einfach in die Protokolldatei.



Die Datei PROTOKOLL MBR(PROTO01)

Die erlösende Meldung steht in Zeile 14: Transfer complete.

5.4.3 Der Domain Name Service (DNS)

Ein Merkmal des TCP/IP-Netzwerks besteht darin, dass sämtliche für den Transport von Datenpaketen erforderlichen Adressen numerisch gestaltet sind. Aus Gründen, die auf der Hand liegen, hat man sich schon frühzeitig darum bemüht, sozusagen als Stellvertreter für numerische Adressen namensbezogene Adressen zu vergeben. In den frühen TCP/IP-Implementationen war für die Umsetzung von numerischen Adressen in Namen die Datei HOSTS zuständig (siehe Kapitel: 5.3.4).

Die Verwendung der Datei HOSTS bringt sowohl Vorteile als auch Nachteile mit sich. Ein Vorteil besteht sicherlich in der einfachen Handhabung dieser Datei. Lediglich ein Texteditor ist notwendig, um die Datei zu bearbeiten. Die Einträge, die hinterlegt werden müssen, haben einen einfachen und logischen Aufbau. Als gravierender Nachteil kann angesehen werden, dass die Datei HOSTS ein lokales Objekt jedes TCP/IP-Hosts ist. Jeder Host, der eine Adressumsetzung für sich durchführen soll, muss eine eigene Datei HOSTS besitzen, die darüber hinaus auch noch einen bestimmten Standort in der Verzeichnisstruktur eines jeden Hosts besitzen muss. Ein Netzwerkverzeichnis verbietet sich von vornherein für die Datei HOSTS.

Stellen Sie sich einmal vor, dass Sie 300 TCP/IP-Host zu administrieren haben, die jeder eine eigene Datei HOSTS besitzen. Wenn jetzt die Forderung besteht, dass alle diese Datei den gleichen Inhalt haben, so ist die Vorstellung nicht abwegig, dass es irgendwann zu Asynchronitäten in diesem Konstrukt geben wird. Denken Sie an Murphy: was geschehen kann, wird auch irgendwann geschehen.

Aus diesem Mangel in der Verwendung der Datei HOSTS hat sich die Entwicklung des Domain Name Service (DNS) ergeben.

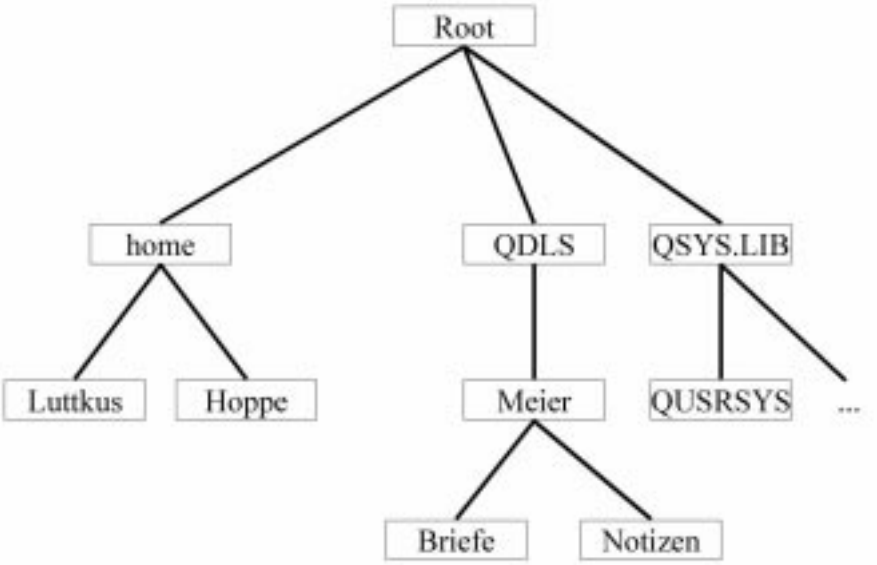
Dieser Dienst ermöglicht Anwendungen, die miteinander über die Socket-Schnittstelle des TCP/Ips kommunizieren, Host-Namen einfach auszuwerten, indem sie eine Adressabfrage an einen zentralen Server senden.

5.4.3.1 Überblick über den DNS

Der Domain Name Service, kurz DNS genannt, wurde bereits 1983 als Standard eingeführt und steht als Dienst des OS/400 seit Version 4 Release 2 den AS/400 Anwendern zur Verfügung. Im Gegensatz zur flachen Struktur der Datei HOSTS, werden die Host-Namen vom Domain Name Service in einer hierarchischen Datenbank verwaltet, die durchaus im Netzwerk verteilt verwaltet werden kann. Bevor ich jedoch in die Konfiguration des Domain Name Service der AS/400 einsteige, möchte ich jedoch mit Ihnen einige Grundlagen des Domain Name Service betrachten. Diese Grundkenntnisse ermöglichen Ihnen dann, die Konfigurationsgänge besser zu verstehen.

5.4.3.1.1 Hierarchien

Allgemeine Formen hierarchischer Datenverwaltungen sind Ihnen sicherlich bekannt. Hierarchische Verzeichnisstrukturen werden von fast allen derzeit geläufigen Betriebssystemen verwendet – DOS, Windows, Netware, UNIX, OS/400 (seit V3R1). Diese die Datenhaltung beschreibenden Strukturbäume stehen immer auf dem Kopf und werden deshalb auch inverse Bäume (inverted trees) genannt.



Eine einfache Hierarchie

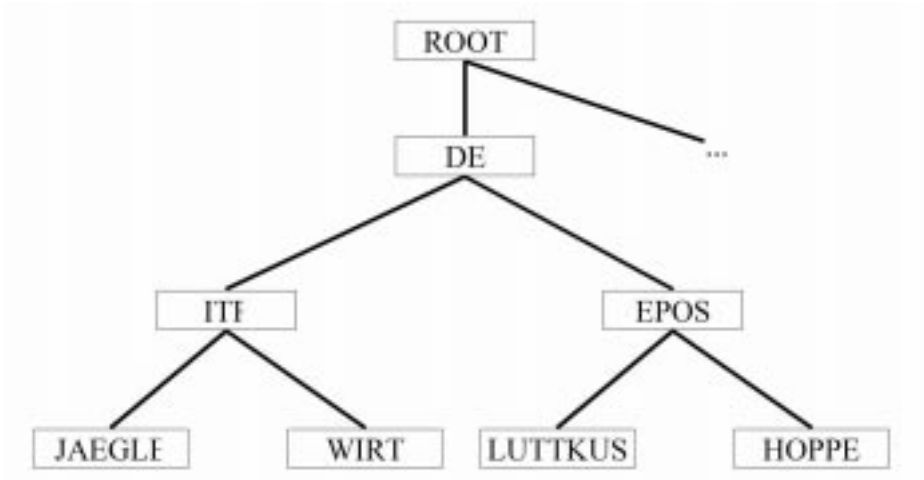
In einem inversen Baum repräsentieren die Schnitt- und Endpunkte (Kästen) der Struktur die Daten. Diese Punkte werden Knoten oder auch nodes genannt. Mit Hilfe eines voll qualifizierten Na-

mens kann jeder Knoten im Baum eindeutig angesprochen werden. Der voll qualifizierte Name wird auch als Pfad (path) bezeichnet. Möchte ich mit Daten im Verzeichnis Notizen arbeiten, so spreche ich sie unter dem eindeutigen Pfad \QDLS\MEIER\NOTIZEN an.

Eine wichtige Hierarchieregel sollten Sie nie außer acht lassen! Knoten gleicher Hierarchieebene dürfen niemals einen identischen Namen haben. Es darf nicht unterhalb des Knotens MEIER einen zweiten Knoten mit dem Namen MEIER geben.

5.4.3.1.2 Der Domain Name Space

Die hierarchische Datenbank des Domain Name Service wird als Domain Name Space bezeichnet. Jeder der im Domain Name Space verzeichneten Hosts hat einen eindeutigen voll qualifizierten Namen.



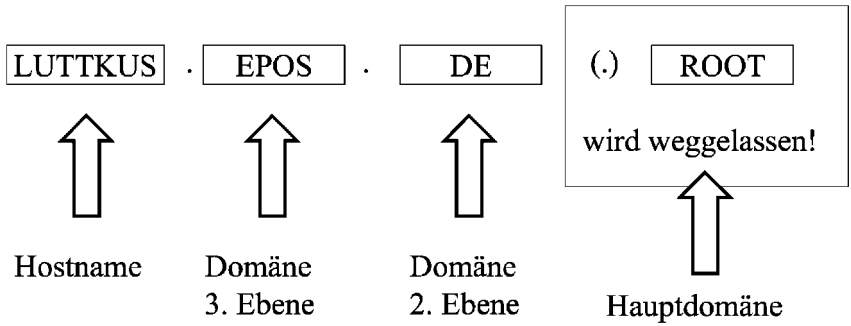
Ein DNS-Baum

Das Root-Verzeichnis einer Domäne wird allgemein als Hauptdomäne bezeichnet. Jeder Knoten im Baum erhält einen Namen, der aus maximal 63 Zeichen bestehen kann. Jeder Knoten wird durch einen voll qualifizierten Namen beschrieben. Im Gegensatz zu einem Verzeichnisbaum beginnt die Beschreibung des voll qualifizierten Namens nicht mit dem Root (der Hauptdomäne), sondern mit dem Namen des in Frage kommenden Knotens und endet mit der Hauptdomäne. Die einzelnen Domänenknoten werden durch Punkte voneinander getrennt.

In oben gezeigten Bild wäre ein Beispiel für eine voll qualifizierte Domäne folgende Angabe:

LUTTKUS.EPOS.DE

Eigentlich müsste noch ein Punkt als Trennzeichen für die Hauptdomäne angegeben werden, dieser wird jedoch im Allgemeinen weggelassen.



Auswertung des Namenseintrags

Der hier gezeigte Domänenname lässt folgende Interpretation zu:

- LUTTKUS ist der Name eine Systems (HOSTS) in der Domäne EPOS, die wiederum Bestandteil der nationalen Domäne DE ist.

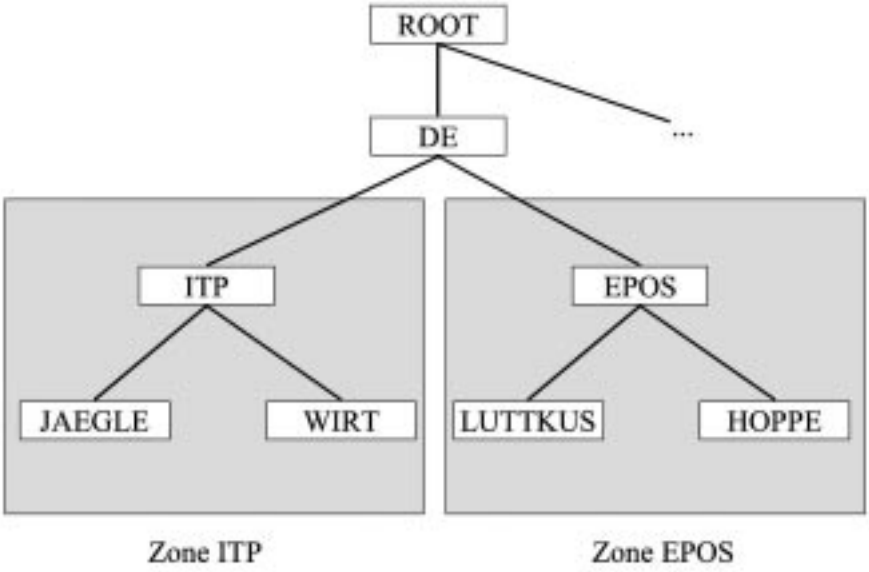
Achtung: Rein theoretisch wäre auch folgende Interpretation zulässig: Die Domäne LUTTKUS ist Bestandteil der Übergeordneten Domäne EPOS, die wiederum Bestandteil der nationalen Domäne DE ist.

Welche der genannten Interpretationen richtig ist, setzt genaue Kenntnisse über die jeweilige Domäne voraus und kann nicht dem Namen allein entnommen werden.

5.4.3.1.3 Die Zone

Der Domain Name Service wurde entwickelt, um das Internet insgesamt besser verwalten zu können. Dieses ist jedoch zu umfangreich, um von einem einzigen Punkt zentral verwaltet werden zu können. Deshalb hat man die Verwaltung von Subdomänen an untergeordnete Namensserver übergeben.

Namensserver (auch Domain Name Server) sind Programme, die einen Domain Name Space verwalten. Dabei kann der gesamte Verwaltungsbereich in sogenannte Zonen unterteilt werden.



Aufteilung einer Domäne in Zonen

Eine Zone stellt die Untermenge eines Domain Name Space-Baums dar. Wobei dann ein Namens Server für eine oder mehrere Zonen zuständig sein kann.

5.4.3.1.4 Warnung: Der Domänenbegriff

Ich möchte Sie dringend bitten, einen Sachverhalt zu berücksichtigen. Als Netzwerkadministratoren in einem heterogenen Netzwerk, welches unterschiedliche System beinhaltet, werden wir öfter mit dem Begriff der Domäne konfrontiert, vor allen Dingen aber dann, wenn wir mit Microsoft Betriebssystemen arbeiten müssen.

Das Microsoft-Netzwerk verwendet ebenfalls den Begriff der Domäne, jedoch in einem komplett anderen Kontext als im TCP/IP-Netzwerk:

Im Microsoft-Netzwerk beschreibt eine Domäne einen bestimmte Anzahl von Systemen, die über eine gemeinsame Sicherheitsdatenbank verwaltet werden. Es kann also durchaus geschehen, dass Host, die in **verschiedenen** Microsoft Domänen verwaltet werden Bestandteil **einer** TCP/IP-Domäne sind.

Fazit:
Die Domänenbegriffe dieser beiden Netzwerkwelten haben nichts miteinander zu tun!

5.4.3.2 Der AS/400 Domain Name Service

Ab OS/400 V4R2 sind auf dem System IBM AS/400 zwei DNS-Server verfügbar. Der eine DNS-Server ist ein auf dem System IBM AS/400 ausgeführter Basis-Server. Dieser DNS-Server ist als Option 31 von OS/400 (5769-SS1) mit der Bezeichnung „OS/400-Domain Name System“ verfügbar.

Beabsichtigen Sie, den Domain Name Service auf der AS/400 zu nutzen, so sollten Sie sicherstellen, dass die Komponente 31 des Betriebssystem (5769-SS1) bereits installiert ist. Sollte dieses nicht der Fall sein, so muss diese Komponente nachinstalliert werden. Verwenden Sie hierfür den Befehl RSTLICPGM oder alternativ das LICPGM-Menü und dann die Option 11 Lizenzprogramm installieren. Mit dem Befehl CHKPRDOPT sollten Sie sodann überprüfen, ob die Installation korrekt vollzogen wurde.

Alle vom DNS der AS/400 erzeugten Konfigurationsdateien werden direkt im Integrated File System der AS/400 abgelegt und zwar in folgendem Zweig:

/QIBM/UserData/OS400/DNS

Für die Konfiguration des Dienstes sind folgende Sonderberechtigungen notwendig:

*ALLOBJ

*IOSYSCFG

Um Berechtigungsproblemen aus dem Weg zu gehen, sollten Sie als ein Benutzer der Berechtigungsklasse *SECOFR auf der AS/400 angemeldet sein.

Der andere DNS-Server ist Teil des Lizenzprogramms IBM Firewall für AS/400 (5769-FW1). IBM Firewall für AS/400 ist ein Softwareprodukt, mit dem ein integrierter PC-Server als Firewall eingesetzt werden kann

In den folgenden Abschnitte wird ausschliesslich auf den im Betriebssystem der AS/400 befindlichen Domain Name Service Bezug genommen.

5.4.3.2.1 Der Operations Navigator

Die Installation und Konfiguration eines DNS-Servers kann komplex sein. Jedoch beinhaltet der Operations Navigator des Client Access einige Wizzards und Assistenten, die die Anfangskonfiguration des AS/400-Domain Name Service stark vereinfachen.

Der Operations Navigator stellt die einzige verfügbare Schnittstelle für den DNS-Server bereit. Es gibt derzeit keine CL-Befehle die die komplette Konfiguration eines Domain Name Service aus der 5250-Bildschirmschnittstelle heraus ermöglichen.

Die Unterstützung des DNS-Servers durch Operations Navigator bietet mehrere Vorteile:

- Der Assistent für DNS-Konfiguration von Operations Navigator liefert einen einfachen Prozess für die ersten Konfigurations- und Arbeitsschritte zum DNS-Server. Das System erstellt automatisch die vielen Dateien, die für Konfiguration und Betrieb eines DNS-Servers erforderlich sind.
- Die Funktion „Domänendaten importieren“ von Operations Navigator bietet eine Möglichkeit, vorhandene DNS-Server-Konfigurationsdateien in Dateien umzusetzen, die in der Anzeige „DNS-Konfiguration“ von Operations Navigator verwaltet werden können.
- Außerdem können AS/400-Host-Tabelleneinträge in Dateien umgesetzt werden, die in der Anzeige „DNS-Konfiguration“ von Operations Navigator verwaltet werden können.
- Normalerweise werden durch den Domain Name Service Hostnamen in numerische Adressen umgesetzt. Operations Navigator stellt eine Methode für das automatische Aktualisieren von primären Domänendateien mit umgekehrter Zuordnung (IP-Adresse zu Host-Name) mit einem PTR-Ressour-

ceneintrag bereit. Diese umgekehrte Richtung der Adressauflösung wird für einige TCP/IP-Dienste benötigt. Das System führt diesen Schritt aus, wenn zu einer primären Domänendatei mit normaler Zuordnung (Host-Name zu IP-Adresse) ein Eintrag hinzugefügt wird.

5.4.3.2.2 Die Konfiguration des Domain Name Service

Für die Anfangskonfiguration unseren Domain Name Service vergegenwärtigen wir uns folgende Szene: Wir haben ein einfaches nicht allzu großes TCP/IP-Netzwerk. Bestandteil dieses Netzwerks sind 50 PCs, die unter Windows 95, 98 und NT laufen. Derzeit wird die Zugangsberechtigung zum Netzwerk nicht durch einen Windows-NT-Server gesteuert. Zentrales Serversystem in unserem Netzwerk ist eine AS/400 neueren Baujahrs. Diese AS/400 wird als Applikationsserver – 5250-Anwendungen – und als File-Server für alle PC-Dateien eingesetzt. Diese Daten werden durch Office Anwendungen (Winword, Excel etc.) erzeugt und direkt im ASCII-Bereich des Integrated File Systems gehalten. Eine lokale Datenhaltung ist nicht vorgesehen. Bisher wurde hauptsächlich mit numerischen IP-Adressen gearbeitet, bei einigen Systemen wurden auch Hosttabellen eingesetzt. Um eine einfacherer Administration zu ermöglichen, soll jetzt die AS/400 als Domain Name Server eingesetzt werden.

Da alle PC-Systeme auf die AS/400 als zentrales System via Client Access zugreifen, soll dieser Zugriff in einem ersten Arbeitsgang ermöglicht werden. Folgender voll qualifizierter Name wurde für die AS/400 festgelegt:

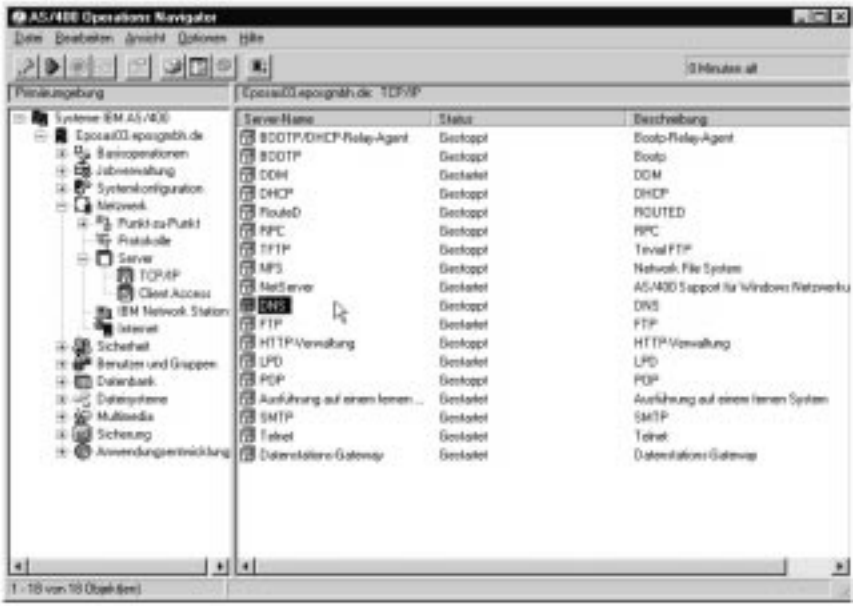
EPOSAS03.EPOSGMBH.DE

Die Schnittstelle für diesen Host wurde mit der IP-Adresse 172.16.0.3 gebunden.

Lassen Sie uns mit der Konfiguration beginnen, indem wir den Operations Navigator (OA) vom Desktop unseres PCs aus aufrufen. Seit Version 3.2.0 des Client Access wird der Aufruf des OA mittels eines gelben Kompass-Icons dargestellt.

Sobald der OA aufgerufen wurde, müssen Sie das Maschinensymbol für die AS/400 expandieren. Öffnen Sie sodann den Knoten Netzwerk, dann den Knoten Server und markieren Sie dann durch einen Doppelklick den Knoten TCP/IP. Nach kurzer Zeit baut sich dann im linken Fensterbereich eine Liste aller auf dem System verfügbaren TCP/IP-basierten Serverprogramme auf.

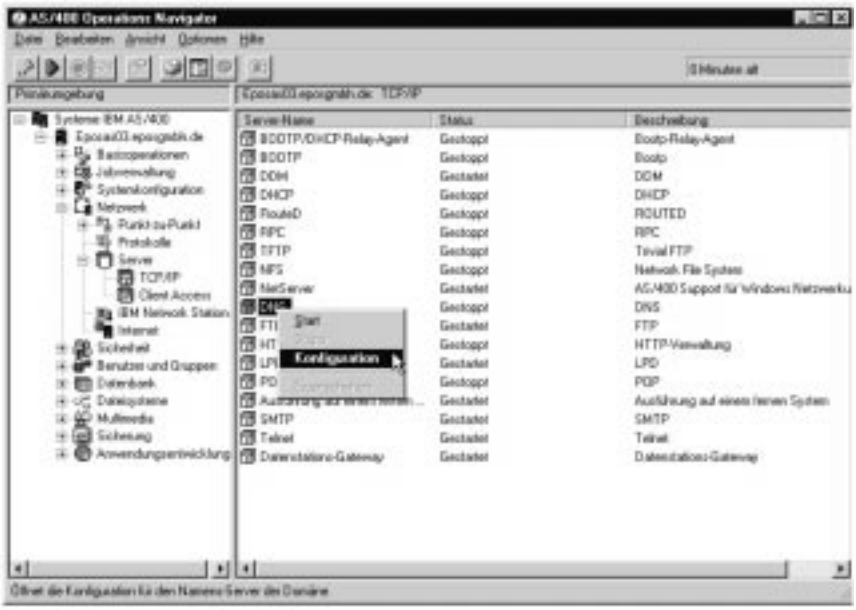
Jetzt sollten Sie einen Eintrag für den AS/400-Domain Name Service sehen. Ist dies nicht der Fall, so müssen Sie die Betriebssystemkomponente 31 (s. o.) nachinstallieren.



Der Domain Name Service ist installiert

Wir sehen hier, dass der Domain Name Service vorhanden ist, er ist derzeit jedoch nicht gestartet. Ein Start des Dienstes ergibt auch keinen Sinn, denn bisher wurden auch keine Einträge in den Domain Name Space gemacht.

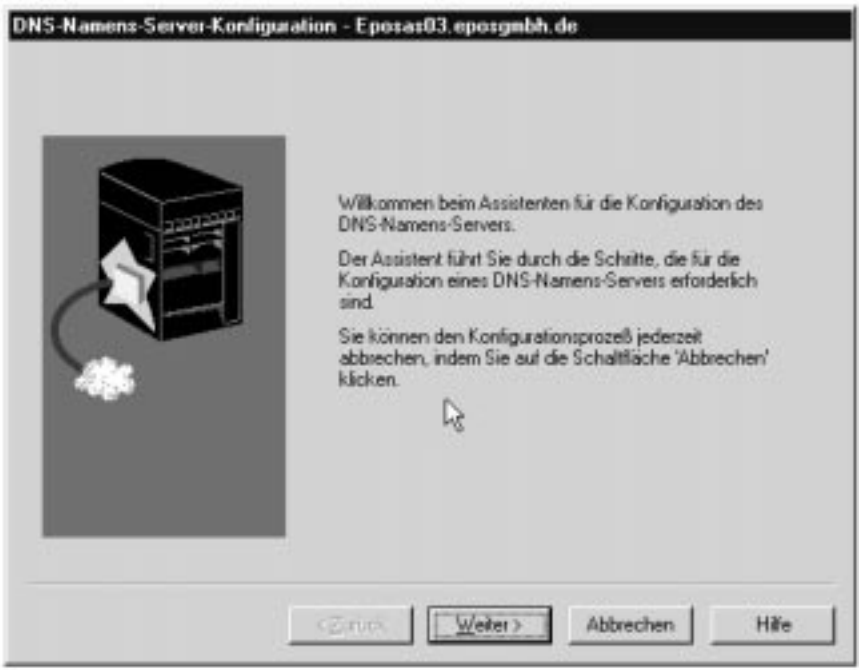
Ich markiere jetzt den Eintrag DNS mit der rechten Maustaste. Es öffnet sich folgendes Kontextmenü:



Beginn der Konfiguration

Durch Auswahl des Menüpunkts Konfiguration beginnt der Konfigurationsdialog. Bedingt durch den Umstand, dass der DNS-Dienst bisher weder aktiv noch konfiguriert war, wird jetzt automatisch der Konfigurationsassistent des Operations Navigators aktiv, der uns praktisch durch den Konfigurationsdialog führt.

Sie sehen hier abgebildet den Begrüßungsdialog des DNS-Assistenten.



Willkommen!

Ich bestätige diesen ersten Dialog mit Weiter und der erste Konfigurationsdialog öffnet sich.

In diesem Dialog wird von erwartet, dass hier der TCP/IP Host benannt wird, auf dem der DNS-Dienst sein aktiv wird. Im TCP/IP-Jargon wird dieser Host als sogenannter Root-Server bezeichnet.

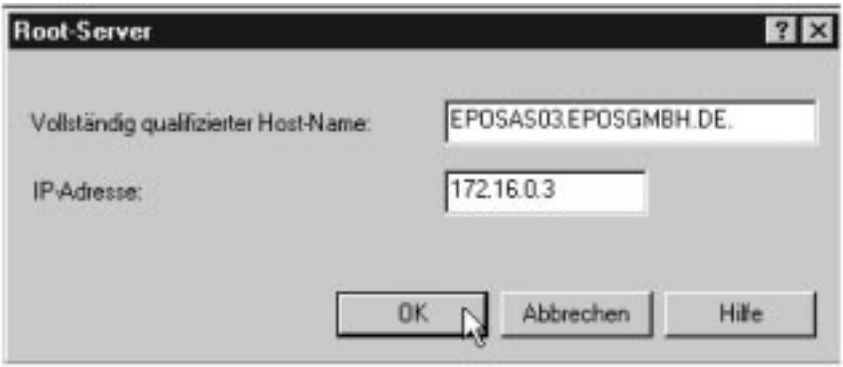
Hinzufügen des Root-Server 1

Betätigen Sie jetzt den Hinzufügen-Knopf und folgendes Fenster öffnet sich:

Hinzufügen des Root-Servers 2

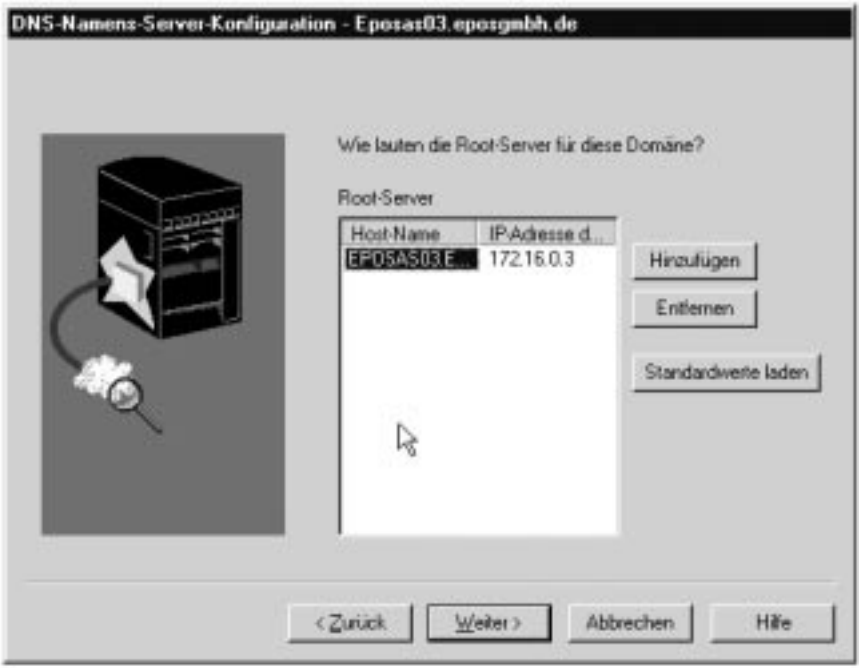
Da wir für unsere AS/400 bereits einen Hostnamen haben (s. o.) tragen wir folgende Werte in die Eingabefelder ein:

- Vollständig qualifizierter Host-Name:
  EPOSAS03.EPOSGMBH.DE
- IP-Adresse:
  172.16.0.3



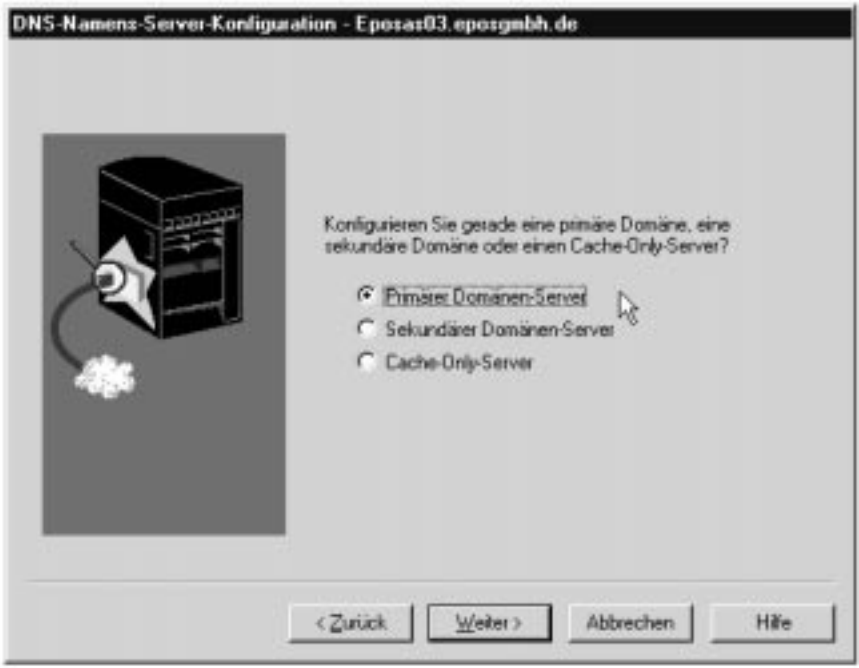
Werte bestätigen

Durch Drücken des Knopfes OK werden diese Eingaben bestätigt. Daraufhin erscheinen diese Werte im Ausgangsdialog wie folgt:



Der Root-Server wurde eingetragen

Achtung: Wir haben jetzt lediglich definiert, welches sozusagen der gastgebende Server für den DNS-Dienst unseres Netzwerks ist. Wir haben jedoch noch keinen Eintrag hinterlegt mittels dessen eine Namens- bzw. Adressauflösung getätigt werden kann. Diese Einträge müssen noch später erfolgen. Also wir sind noch lange nicht am Ende.



Definition des Primären Domänen-Servers

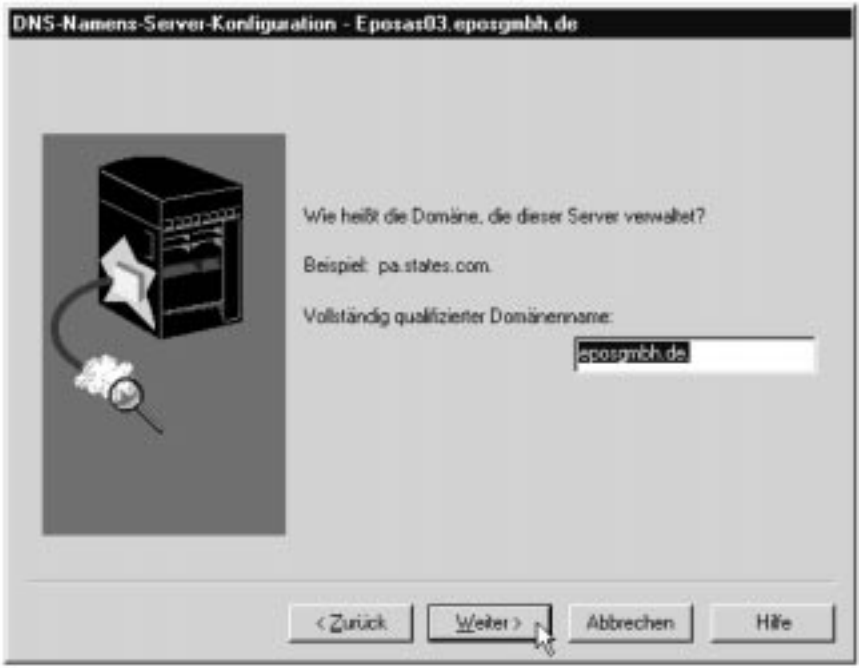
Da dieses der erste DNS ist, der von uns definiert wird, muss hier der Parameter Primärer Domänen-Server markiert werden. Ein primärer Namensserver lädt die Informationen eines Berechtigungsbereichs von der Platte und hat die Berechtigung für den in der Plattendatei angegebenen Berechtigungsbereich.

Ein sekundärer Namensserver hat die Berechtigung für einen Berechtigungsbereich, erhält die Informationen zu seinem Berechtigungsbereich jedoch von einem primären Server. Dieser Prozess wird Übertragung des Berechtigungsbereichs genannt. Um die Synchronisation zwischen sekundären und primärem Server aufrechtzuerhalten, senden die sekundären Namensserver

regelmäßig (in der Regel alle drei Stunden) Anfragen an den primären Namens-Server. Die Übertragung des Berechtigungsbereichs wird erneut ausgeführt, wenn der primäre Server aktualisiert wird. Die Definition eines sekundären Namensservers ist eine Absicherung gegen des Ausfall des primären Domänen-Servers. Sollte der primäre Server ausfallen, so übernimmt der sekundäre Server dessen Aufgaben.

Ein Namensserver, der keine Berechtigung für einen Berechtigungsbereich hat, wird als Cache-Only-Server bezeichnet. Ein Cache-Only-Server erhält alle angeforderten Daten von primären oder sekundären Namens-Servern. Ein solcher Server benötigt mindestens einen Root-Server, um auf einen Namensserver zu zeigen, von dem er Informationen erhalten kann

Im nächsten Dialog muss der vollständig qualifizierte Domänenname eingegeben werden, für den der DNS die Verwaltung übernehmen soll.



Der vollständig qualifizierte Domänenname

Der von uns verwendete Hostname für die AS/400 war:

EPOSAS03.EPOSGMBH.DE

Dieser Name besteht aus vier Komponenten. Ich habe mich nicht verzählt, Sie sehen zwar drei Komponenten, eine vierte ist praktisch unsichtbar.

1. EPOSAS03: der Hostname
2. EPOSGMBH: die Domäne der dritten Ebene
3. DE: die Domäne der zweiten Ebene
4. nicht sichtbar: die Hauptdomäne

Sollten Sie sich hier noch unsicher sein, so lesen Sie bitte noch einmal den Abschnitt 5.4.3.1.2 durch!

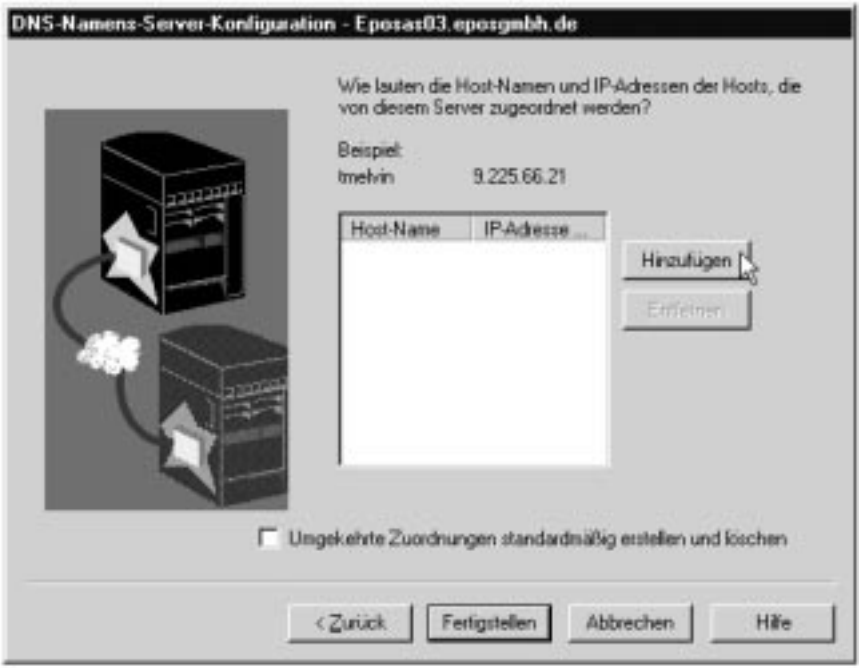
Was müssen wir also für den voll qualifizierten Domänennamen jetzt eingeben?

EPOSGMBH.DE.

Vergessen Sie nicht den abschliessenden Punkt, ansonsten erhalten Sie eine Fehlermeldung!

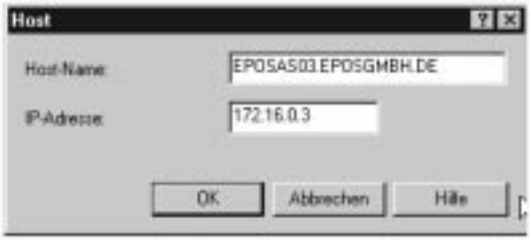
Ich beende den Dialog mit dem Weiter-Button.

Der letzte Schritte ist jetzt leicht erledigt. Denn jetzt muss der Host, für den eine Namensauflösung realisiert werden soll, eingetragen werden.



Einen Host in den Name Space eintragen

In diesem Dialog drücke ich den Hinzufügen-Knopf und folgendes Bild erscheint:

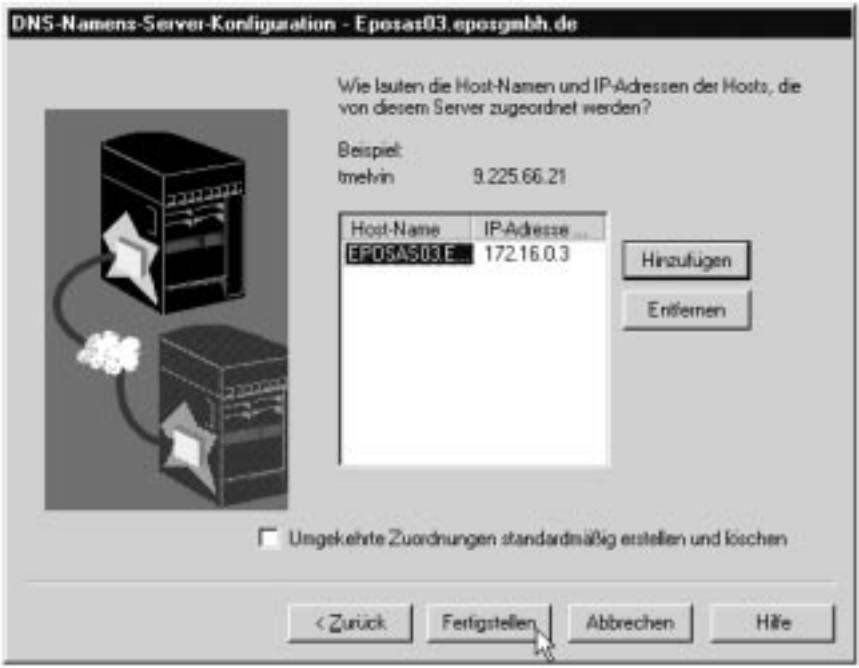


Die AS/400 als Ziel-Host eintragen

Ich trage den Hostnamen der AS/400 – EPOSAS03.EPOSGMBH.DE – und die IP-Adresse 172.16.0.3 in diesen Dialog ein.

Da in unserem Netzwerk derzeit die AS/400 der einzige Host mit Serverfunktionen ist, ist sie das einzige System, welches als Ziel für Serveranforderungen betrachtet werden kann. Alle anderen Host unseres TCP/IP-Netzwerks sind lediglich Clients der AS/400 und somit in den Kommunikationsanforderungen nur als Quellsystem anzusehen. Deshalb ist es vorerst auch nur nötig, die AS/400 als Host in den DNS-Dienst aufzunehmen.

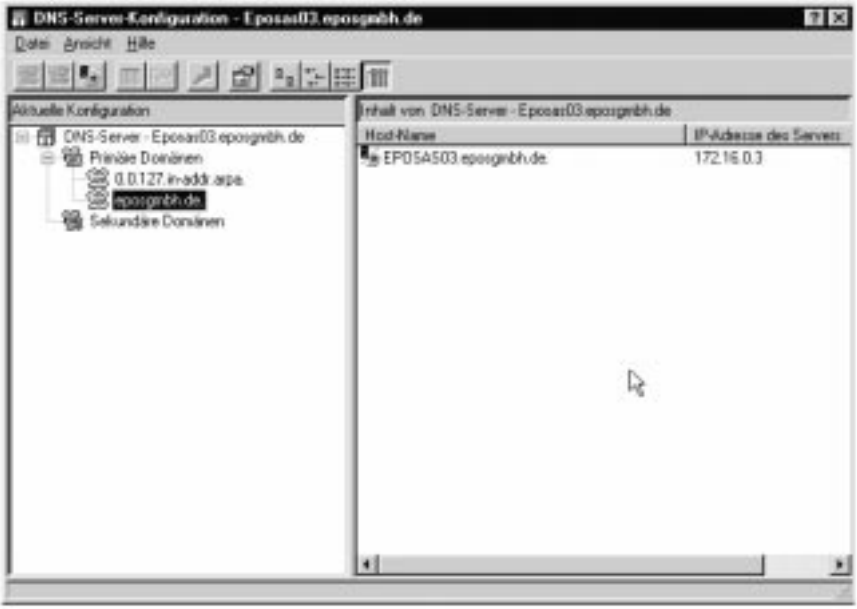
Nachdem ich diesen Dialog mit OK beendet habe, wird das folgende Fenster angezeigt:



Der Host ist eingetragen

In diesem Dialog wird jetzt angezeigt, dass der Host EPOSAS03.EPOSGMBH.DE in den Name Space des DNS aufgenommen wurde. Damit ist eine Auflösung des Namens in eine numerische Adresse möglich. Sollte jetzt z. B. für Mail-Dienste eine umgekehrte Auflösung – von der numerischen Adresse zum Namen ermöglicht werden – so sollte jetzt der Parameter „Umgekehrte Zuordnung standardmäßig erstellen und löschen" markiert werden.

Mit Fertigstellen beenden Sie den Dialog. Daraufhin erscheint das „richtige" Konfigurationsfenster. Jegliche weitere Konfigurationsarbeit wird aus diesem Dialog heraus wahrgenommen.



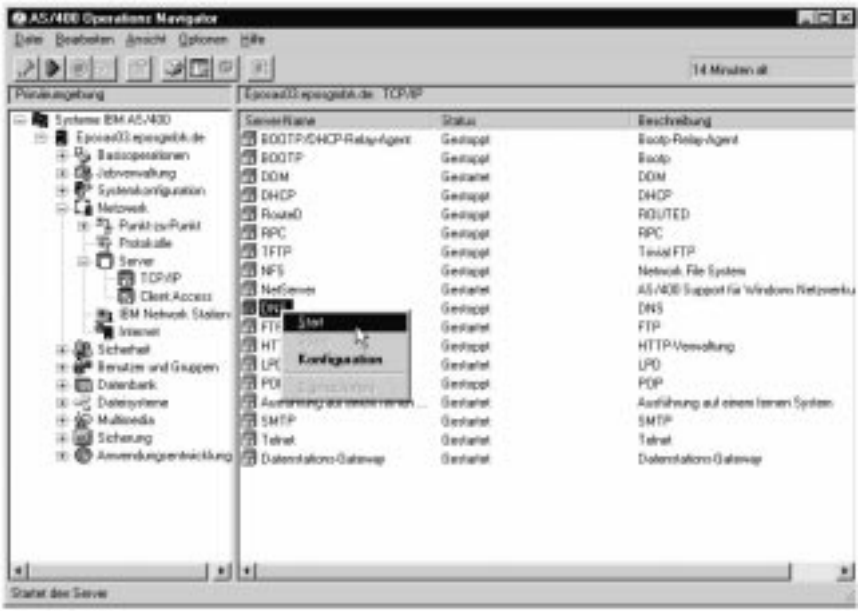
Der Konfigurationsdialog

Was wird hier dargestellt? Betrachten wir zuerst den linken Bereich des Fensters. Hier wird die aktuelle Konfiguration angezeigt. Wir sehen folgende Bestandteile der Konfiguration als Verzeichnisstruktur:

- den Root-Server: DNS-Server – EPOSAS03.EPOSGMBH.DE
- die Primäre Domäne
- einen Namespace für die Adressauflösung zum Namen: 0.0.127.in-addr-arpa
- einen weiteren Namespace für unsere Domäne: EPOSGMBH.DE. Hierüber wird die Namensauflösung zur Adresse realisiert.

Wenn wir den Eintrag für die Domäne EPOSGMBH.DE markieren, wird auf der rechten Seite des Konfigurationsfensters, die bereits eingetragenen Hosts angezeigt. In unserem Fall der Host EPOSAS03.EPOSGMBH.DE

Verlassen Sie jetzt den Konfigurator und Sie kehren in das Hauptfenster des Operational Assistant zurück.



Den DNS starten

Mit Hilfe des Kontextmenüs und der Auswahl Start wird der DNS gestartet.

5.4.3.2.3 Weitere Hosts in den DNS eintragen

Nachdem jetzt die Schnittstelle unsere AS/400 unter dem Namen EPOSAS03 angesprochen werden kann, widmen wir uns der Aufnahme weiterer Hosts in die Zonendatei des von uns konfigurierten DNS-Servers.

Lassen Sie uns zuerst die Frage stellen, welche Hosts überhaupt mit Hilfe des DNS-Dienstes angesprochen werden sollen. Grundsätzlich läßt sich Folgendes sagen: Es macht eigentlich nur Sinn, Zielhosts in die Zonendatei aufzunehmen. Verstehen wir unsere AS/400 als zentralen Server in unserem Netzwerk, der Applikationsserver, Fileserver, Kommunikationsserver etc. ist, so betrachten wir dieses System sicherlich als einen Zielhost, der uns zentral Ressourcen zur Verfügung stellt.

Meistens ist unser Netzwerk jedoch nicht so strikt zentralisiert. Wir haben z. B. ein oder mehrere NT-Server in unserem Netzwerk, die für die Berechtigungssteuerung, den Backup von Berechtigungsdaten und das Versorgen mit Windows-Anwendungen zuständig sind. Möglicherweise tut dann auch noch ein Linux-System seine Dienst als Kommunikationsserver, dann haben wir auch noch einen RS6000-Rechner, auf dem Lotus Domino installiert ist usw.

Die Folge davon ist, dass wir nicht nur unsere AS/400 als Ziel-Host in unseren Domain Name Service eintragen müssen, sondern auch noch diverse andere Server-Systeme.

An dieser Stelle setzen wir jetzt ein. Stellen Sie sich folgenden Sachverhalt vor:

Neben dem AS/400 System EPOSAS03 mit der IP-Adresse 172.16.0.3 existiert noch ein Windows NT Server als Applika-

tionsserver. Dieser Server versorgt das gesamte Netzwerk mit Windows Applikationen wie Winword, Excel, Powerpoint etc. Auch dieses System wird zentral von allen Clients als Zielserver angesprochen und soll mit Hilfe des DNS-Dienstes auf der AS/400 angesprochen werden können.

Folgende Werte/Eckdaten müssen uns bekannt sein:

- die IP-Adresse,
- der Name, der für den neuen Host zu verwenden ist.

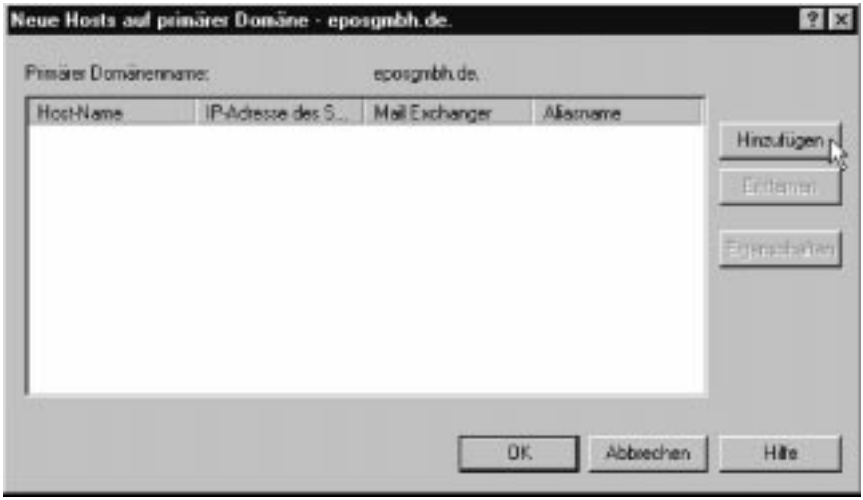
Der Name des NT-Servers wird von uns mit TSESERVER festgelegt, die IP-Adresse für unser Beispiel lautet 172.16.0.5.

Jetzt beginnt die Konfiguration. Rufen Sie den Operations Navigator auf, gehen Sie über das Symbol Netzwerke in den Bereich TCP/IP, dann in den Bereich SERVER und öffnen Sie sodann den DNS-Dienst durch Doppelklick. Nachdem sich der DNS-Dienst-Explorer geöffnet hat, sehen Sie auf der rechten Seite des DNS-Explorers, die bereits in den DNS-Dienst aufgenommenen Hosts. In unserem Falle lediglich den Hostnamen und die IP-Adresse des bisher eingetragenen Hosts.

Gehen Sie jetzt mit der Maus in den leeren Bereich des rechten Explorer-Fensters und betätigen Sie die rechte Maustaste. Folgendes Fenster öffnet sich:

Einen neuen Host aufnehmen – 1

Wählen Sie im gezeigten Kontextmenü den Punkt Neuer Host mit einem Doppelklick aus und der jetzt angezeigte Dialog öffnet sich:



Einen neuen Host aufnehmen – 2

Klicken Sie jetzt auf Hinzufügen und der eigentliche Konfigurationsdialog für die Aufnahme eines neuen Host in den DNS-Dienst der AS/400 beginnt.

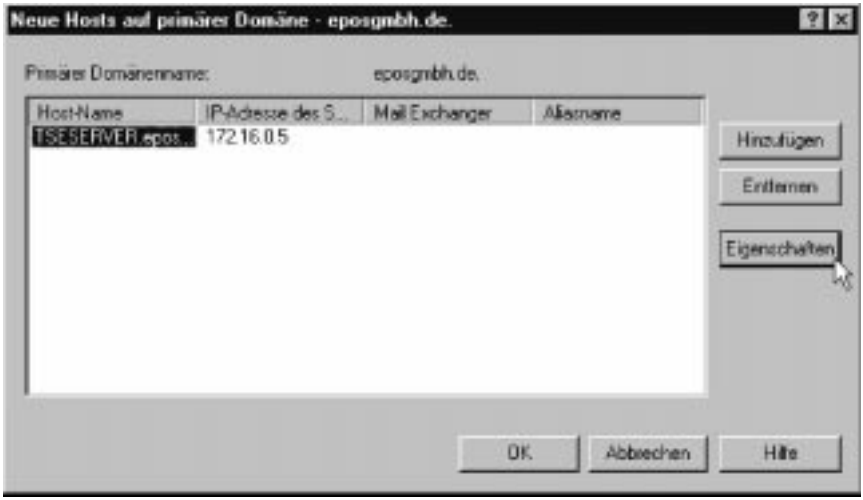
Adresswerte versorgen

In diesen Dialog tragen wir folgende Werte ein:

Host-Name: TSESERVER

IP-Adresse: 172.16.0.5

Die anderen Werte interessieren uns an dieser Stelle nicht und deshalb wird der Dialog mit OK bestätigt und beendet. Jetzt erscheint ein Fenster, das wir eigentlich schon kennen, jedoch beinhaltet dieses Fenster die gerade eingegebenen Daten:



Ein neuer Host wurde in den DNS aufgenommen

Wir sehen hier, dass dem Hostnamen TSESERVER und der Name der Domäne einfach beigefügt wurde und welcher IP-Adresse dieser Hostname entspricht.

Eigentlich könnten wird jetzt schon den Dialog insgesamt mit OK beenden, denn alle zwingend notwendigen Eingaben wurden erledigt. Bevor wir jedoch den Dialog beenden, klicken wir zuerst noch einmal auf den Knopf Eigenschaften, um uns eine Überblick darüber zu verschaffen, welche weiterführenden Einstellungen noch möglich sind.

Wählen Sie den Eigenschaften Dialog an, so öffnet sich folgendes Fenster. Sie sehen, dass dieses Fenster aus mehreren Registratur-Dialogen besteht:

- Allgemein
- Text

- Mail
- Plattform
- Aliasnamen
- Umgekehrte Zuordnung

Register Allgemein

Im Register Allgemein sehen Sie die von uns bisher eingegebenen Adressdaten für den neu eingegebenen Host, jetzt jedoch nicht in verkürzter Form, wie in den bisherigen Dialogen, sondern komplett.

Wir sehen hier den voll qualifizierten Hostnamen des neuen Systems – TSESERVER.EPOSAS03.EPOSGMBH.DE. – und die zugeordnete IP-Adresse 172.16.0.5.

Mit Hilfe des Hinzufügen-Buttons könnten wir jetzt weitere Hosts in den DNS aufnehmen.

Der Parameter Cache-Zeit ist für uns nicht maßgeblich. Es besteht beim DNS-Dienst die Möglichkeit, sogenannte Cache-DNS-Server aufzubauen. Cache DNS-Server dienen dazu häufig angesprochenen Host-Namen und Adressen in den Hauptspeicher des Rechners der den DNS-Dienst ausführt zu übertragen, sodass eine Adressauflösung deutlich schneller ist, verglichen mit einem „normalen" DNS-Dienst, bei dem jeder Adress-Auflösungsprozess einen Zugriff auf den Plattenspeicher auslöst. Ein Cache-DNS-Server kann jedoch nicht allein existieren, sondern kann nur zusätzlich in einer Domäne arbeiten. Deshalb ist dieser Parameter für uns jetzt nicht maßgeblich.

Das Register Text hat eigentlich Kommentierungsfunktionen.

Register Text

Mittels des Hinzufügen-Dialogs können Sie diesem Host-Eintrag jede nur denkbare Textinformation hinzufügen. Es wäre durchaus denkbar und sinnvoll, hier Standortinformationen zu hinterlegen.

Damit wären wir auch schon wieder bei der Diskussion, welchen Host wir in den DNS-Dienst aufnehmen. Vorhin hatten ich gesagt, dass eigentlich nur Zielsysteme eingetragen werden müssten. Diese Argumentation basierte auf dem Gesichtpunkt der technischen Notwendigkeit. Es ist technisch notwendig, nur diejenigen Systeme in diesen Dienst einzutragen, die für das Netzwerk Server-Funktionen wahrnehmen.

Sehen wir uns diesen Dialog mit seine Kommentarfunktionen an, so könnte ich abweichend vom Vorherigen formulieren: Ich nehme **jedes** System als Host in den DNS auf, dann ist es möglich, jeden Host bezüglich Standort, Gerät etc. zu erfassen und zu kommentieren und ich erhalte eine zentrale Netzwerkbeschreibungsdatenbank. Denken Sie einmal darüber nach!

Register Mail

Sollte der gerade eingetragene Host ein Mail-Server sein, so kann der Netzwerkadministrator, sofern in seinem Netzwerk mehrere mail-Server arbeiten, mit Hilfe des Parameters Vorgabe eine Rangfolge der Mail-Server erstellen, so dass Mail-Adressen leichter gefunden werden können.

Auch das Register Plattform hat reine Kommentierungsfunktion.

Register Plattform

Mit Hilfe dieses Registerblatts kann eine technische Beschreibung für jeden verzeichneten Host in der DNS-Datenbank angelegt werden.

Im Register Aliasnamen können für vergebene Hostnamen Aliasnamen hinterlegt werden.

Register Aliasnamen

Im Prinzip könnte man einfach sagen, dieses wäre ein Parameter für die Schreibfaulen unter uns. Durch den erzeugten Hosteintrag in der DNS-Datenbank wird unser NT Server unter dem Hostnamen TSESERVER.EPOSGMBH.DE anzusprechen sein. Es wäre doch schön, wenn wir alternativ einen Kurznamen verwenden könnten, wie z. B. TSE. Sollte das der Fall sein, so würden wir hier mit dem Hinzufügen-Dialog den Namen TSE eintragen

und wir könnten diesen NT-Server einfach mit dem Namen TSE einsprechen. Auch hinter diesem Namen stünde im übertragenen Sinne die IP-Adresse 172.16.0.3.

Aber nur Schreibfaulheit als Grund für die Existenz von Alias-Hostnamen anzuführen wäre nicht genug. Eigentlich steckt vielmehr folgender Sachverhalt dahinter: Wenn ein Serverdienst nicht die Berechtigungsstruktur des OS/400 nutzt, aber die im OS/400 angelegte Netzwerkschnittstelle verwendet, so muss zwischen den Serverdiensten der OS/400-Umgebung und den des „Fremdservers" unterschieden werden. In diesem Fall **muss** mit Aliasnamen gearbeitet werden. Zu Kompliziert? Lassen Sie uns ein einfaches Beispiel zur Erklärung heranziehen.

Nehmen wir einmal folgende Situation an:

Unsere AS/400 ist im DNS der AS/400 mittels des Hostnamens EPOSAS03.EPOSGMBH.DE erreichbar. Hinter diesem Hostnamen steht die IP-Adresse 172.16.0.3.

Wir installieren auf diesem AS/400 – System den Lotus Domino Server. Der Domino Server erhält den Namen EPOSAS03. Da der AS/400 – basierte Dominoserver ausschließlich über TCP/IP angesprochen werden kann, nutzt er in unserem Falle die gleiche Netzwerkkarte wie die restlichen AS/400-Serverdienste.

Was ist daran so bemerkenswert? Wir haben einen Adresskonflikt! Wenn jetzt z. B. ein Client Access Dienst mit Hilfe des Hostnamens EPOSAS03.EPOSGMBH.DE auf die Hostserver der AS/400 zugreifen will, so wird er diese auch finden und mit ihnen arbeiten können. Soweit ist alles im grünen Bereich. Ist jetzt aber ein Lotus Notes Client auf demselben PC installiert, so wird er den Domino-Server mit dem Namen EPOSAS03 suchen. Der Notes Client versucht aber ebenfalls, mittels TCP/IP die Verbindung herzustellen. Der jedoch mit einem Namen arbeitet, der nicht im DNS-Dienst

der AS/400 eingetragen wurde (EPOSAS03), so wird die Meldung zurückgegeben, dass keine Verbindung hergestellt werden konnte. Der Notes Client kann also **seinen** Dominoserver nicht finden.

Tragen wir jedoch den Namen EPOSAS03 als Alias-Namen für den Namen EPOSAS03.EPOSGMBH.DE ein, so kann auch der Lotus Notes Client den Dominoserver finden.

Das letzte Register Umgekehrte Zuordnung ist für das beschleunigte Auffinden von Hosts via DNS äußerst wichtig.

Register Umgekehrte Zuordnung

Einige TCP/IP – Dienste betreiben nicht nur die Auflösung eines Hostnamens in eine IP-Adresse, sondern benötigen die Auflösung einer IP-Adresse in einen Hostnamen.

Hostname	Auflösung	IP-Adresse
EPOSAS03	→	172.16.0.1
EPOSAS03	←	1.0.16.172

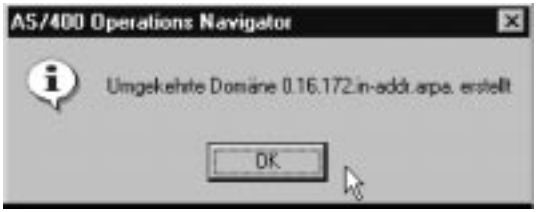
Ich habe diese Vorgänge für Sie noch einmal in der dargestellten kleinen Tabelle aufgezeichnet. Die erste Zeile beschreibt die Adressauflösung in eine IP-Adresse. Die zweite Zeile die Adresse einer IP-Adresse in einen Hostnamen. Achten Sie einmal genau auf die Schreibweise der IP-Adresse. Das ist kein Druckfehler. Die Auflösung der IP-Adresse beginnt mit der Host-ID der gesamten Adresse.

Damit diese umgekehrte Adressauflösung funktionieren kann, muss ein Eintrag für die umgekehrte Zuordnung einer Adresse hinterlegt werden. Diese „umgekehrten Einträge" werden jedoch nicht in die gleiche Zonendatei geschrieben, wie die anfänglich von uns erzeugten Hosteinträge.

Für unseren DNS-Dienst haben wir eine Domäne EPOSGMBH.DE erzeugt, diese enthält alle Hosteinträge für die Auflösung eines Namens in eine IP-Adresse.

Erstellen wir umgekehrte Einträge, so wird eine Domäne mit dem Namen 0.16.172.in.addr.arpa erzeugt. Der numerische Teil dieses Domänennamens ist variabel und hängt von der vergebenen IP-Adresse ab.

Nachdem wir im Register den Punkt Umgekehrte Zuordnungssätze für diesen Host erstellen angeklickt haben und den Dialog mit OK bestätigt haben, erscheint folgende Nachricht:

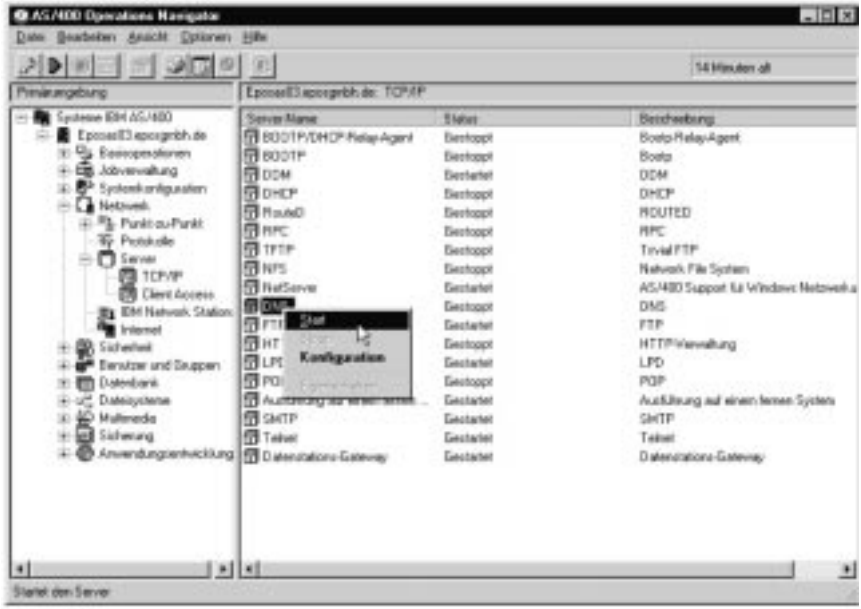


Die „umgekehrte Domäne”

Diese „umgekehrte Domäne” finden Sie dann auch im DNS-Explorer des DNS Dienstes.

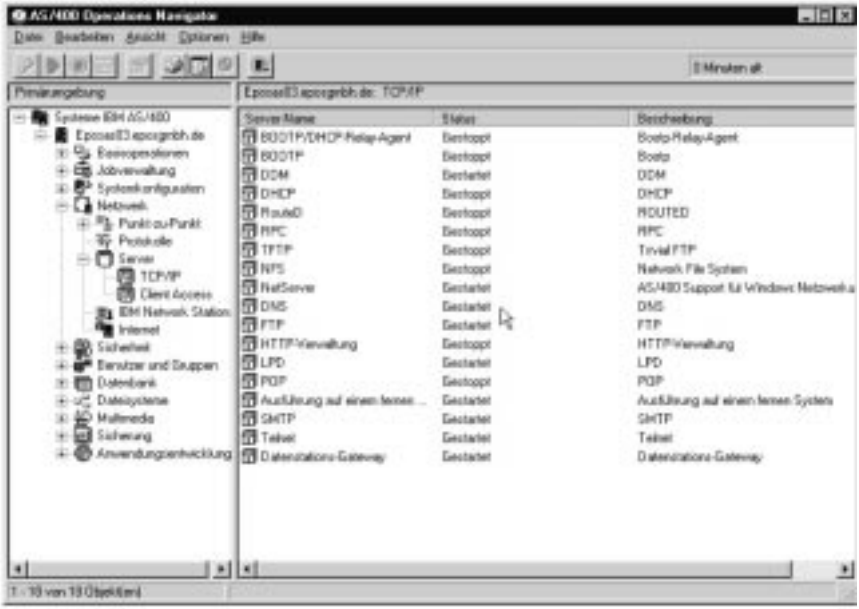
Um jetzt diese neuen Konfigurationswerte in den Serverbetrieb zu übernehmen, gibt es zwei Möglichkeiten:

1. Sie beenden den Betrieb des Servers und starten dann den DNS-Dienst erneut.



Der Server wird erneut gestartet

Achten Sie darauf, dass der Server wirklich gestartet ist!



Der DNS-Server läuft!

Können Sie jedoch nicht den Serverdienst beenden, weil er von Clients benutzt wird und ein Abstellen den gesamten Betrieb in ihrem Unternehmen zusammenbrechen lassen würde, so gibt es noch folgenden Weg:

2. Öffnen Sie den DNS-Explorer und markieren Sie das Symbol für den gesamten DNS. Danach betätigen Sie die rechte Maustaste und wählen dann im Kontextmenü den Punkt Server aktualisieren, sodann werden alle neu konfigurierten Hosteinträge in der DNS Datenbank aktiv.

5.4.3.3 Windows Clients für DNS konfigurieren

Nachdem die Serverdienste konfiguriert wurden, müssen die Clients jetzt für den Betrieb mit dem DNS-Server der AS/400 konfiguriert werden. Solange dieses nicht geschehen ist, kann kein Client auf den DNS-Dienst der AS/400 zugreifen. Jedoch ist die Anbindung eines Windows 95/98/NT-PCs an den DNS Dienst relativ einfach.

Die gesamte Konfiguration erfolgt aus der Netzwerkumgebung des Windows-PCs heraus. Ich markiere also das Symbol Netzwerkumgebung auf dem Desktop meine Windows-PCs. Um diese Umkonfiguration der Netzwerkattribute realisieren zu können, habe ich mich lokal als Administrator angemeldet. Das ist notwendig, da es sich bei meinem Windows-Client um eine NT-Workstation handelt. Beachten Sie, das für diese Arbeit nicht nur das NT-Benutzerkonto Administrator genutzt werden kann. Es kann auch jedes beliebige andere Benutzerkonto genutzt werden, solange es über die lokalen Administrationsrechte verfügt.

Die Windows Netzwerkumgebung

Sodann drücken Sie die rechte Maustaste, markieren den Eigenschaftendialog und öffnen ihn durch Doppelklick.

Die Eigenschaften der Netzwerkumgebung

Jetzt öffnet sich der Netzwerkkonfigurationsdialog. Auch hier werden verschiedene Registerdialoge angezeigt:

- Identifikation
- Dienste
- Protokolle
- Netzwerkkarte
- Bindungen

Für unsere Arbeit benötigen wir lediglich den Dialog Protokolle. Durch einen Klick auf diesen Dialog werden die derzeit für diesen Windows-Client konfigurierten Protokolle angezeigt.

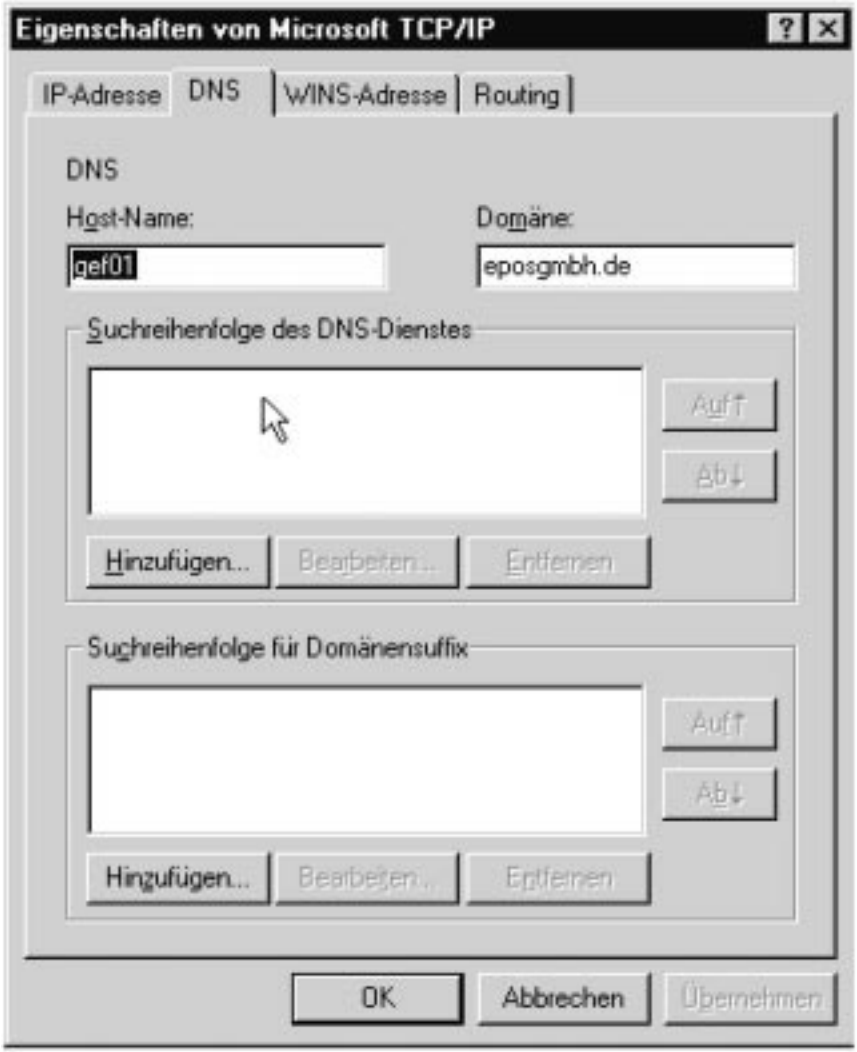
Register Protokolle

Sie sehen, dass für den hier betrachteten Client nur das TXP/IP-Protokoll zur Anwendung kommt. Durch einen Doppelklick auf den Eintrag TCP/IP-Protokoll öffne ich den Eigenschaftendialog.

Auch für diesen Dialog gibt es mehrere Register:

- IP-Adresse
- DNS
- WINS-Adresse
- Routing

Uns interessiert hier das Register DNS:



TCP/IP-Eigenschaften

Was bedeuten folgende Parameter?

Host-Name:
Als Standard steht hier – ohne eigene Konfiguration – der sogenannte Computername des **lokalen Host** (mein PC), der bei der Installation des Windows-PCs angelegt wurde. Sie sehen an dieser Stelle, dass meinem Computer während der Installation der Namen GEF03 gegeben wurde. Tragen Sie hier nie den Hostnamen der AS/400 für das TCP/IP-Netzwerk ein. Das führt zu nichts als Fehlern.

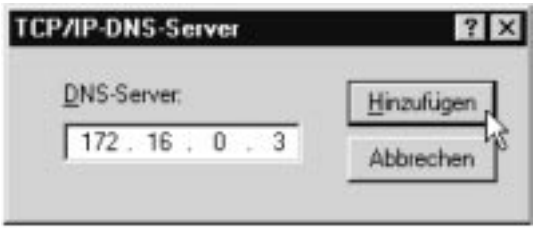
Domäne:
Diesen Parameter belege ich mit dem Domänenname, so wie er im DNS der AS/400 eingetragen wurde. Bitte verwechseln Sie nicht den Domänenbegriff des Microsoft-Netzwerks mit dem des TCP/IP-Netzwerks. Beide Begriffe haben nichts miteinander zu tun. Also tragen Sie hier nicht den Namen der Microsoft Netzwerkdomäne ein. Auch das führt zu nichts, außer zu Fehlern und Missverständnissen.

Wo findet dann dieser Parameter Anwendung, wenn er doch so unwichtig erscheint? Man kann diesen Parameter im Zusammenhang mit dem Alias-Namen im DNS-Dienst sehen. Verwende ich keinen Alias-Namen für den anzusprechenden Server, trage ich hier den Namen der Domäne ein. So kann ich trotzdem mit dem Hostnamen ohne Domänenzusatz eine Verbindung zum Server herstellen.

1. Der qualifizierte Hostname unserer AS/400 war:
   EPOSAS03.EPOSGMBH.DE
2. Im Parameter des Clients steht:
   EPOSGMBH.de
3. Daraus folgt:
   Der Client ist Teilnehmer der Domäne EPOSGMBH.DE

Baue ich eine Verbindung vom meinem Client zur AS/400 auf und benutze nur den Hostnamen der AS/400 EPOSAS03 ohne Domänenzusatz, so wird trotzdem die Verbindung hergestellt, da der Client von sich aus den Domänenzusatz ergänzt.

Jetzt drücke ich im Eigenschaften von TCP/IP-Dialog den Knopf Hinzufügen:



Die Adresse des DNS-Servers

Im Hinzufügen-Dialog muss die Adresse des DNS-Server eingegeben werden. Das ist in unserem Falle die Adresse der TCP/IP-Schnittstelle auf der AS/400: 172.16.0.3 Mit einem Klick auf Hinzufügen wird der Dialog beendet.

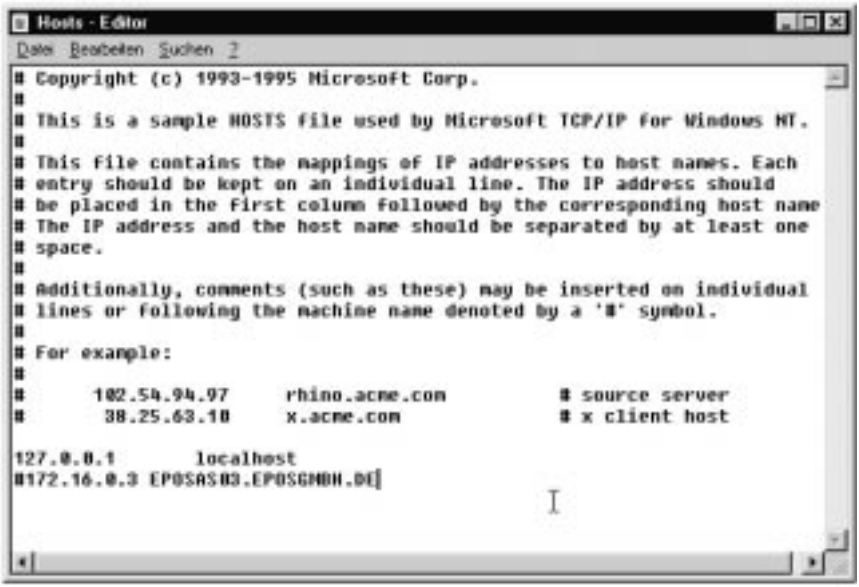
Achtung! Sollten Sie vor der Nutzung des DNS-Servers bereits mit lokalen Hosttabellen gearbeitet haben, so sollten Sie beachten, dass Windows-Systeme grundsätzlich folgende Suchreihenfolge bei der Namens-Adressauslösung berücksichtigen.

- Zuerst in lokaler Hosttabelle suchen.
- Wird dort ein Eintrag gefunden, wird der Namen in die betreffende Adresse aufgelöst.

- Wird der Eintrag nicht gefunden, so wird, falls entsprechend konfiguriert, im DNS nachgesehen, ob hier der entsprechende Namen zu finden ist. Falls dieses der Fall ist wird die IP-Adresse ermittelt.

Um eine aktive Hosttabelle zu deaktivieren, gibt es zwei Möglichkeiten:

1. Löschen Sie die Datei HOSTS. Dieser Schritt ist jedoch für meinen Geschmack etwas zu grobschlächtig. Vielleicht sind einige Server noch nicht Bestandteil des DNS-Dienstes. Sollten Sie also Ihre Datei Hosts löschen, so verlieren Sie vorerst die Verbindung zu den betreffenden Servern.
2. Deaktivieren Sie in der Datei HOSTS den Eintrag für die betreffende Adresse.



IP-Adresse deaktivieren

Ich habe hier den Hosttabelleneintrag dadurch deaktiviert, dass ich vor den Eintrag das Zeichen # (Raute) eingetragen habe. Dieses Zeichen macht die gesamte Zeile zu einer Kommentarzeile.

Sollten dann endlich alle Server in die DNS-Domäne übernommen worden sein, kann ich die Datei HOSTS immer noch löschen.

Nachdem die Konfiguration des Clients beendet wurde, kommt jetzt der Moment der Wahrheit. Mit dem Befehl PING wird jetzt die Verbindung zur AS/400 geprüft.

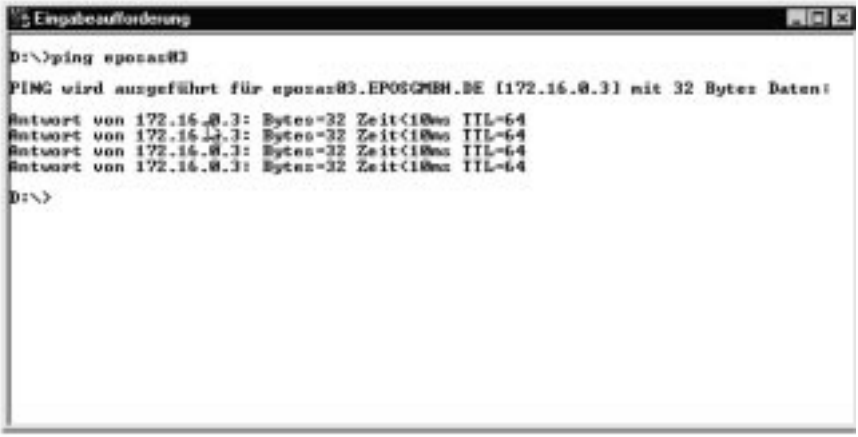
1. PING: mit qualifiziertem Hostnamen
   ping eposas03.eposgmbh.de

1. Erfolgreicher PING

Sie sehen das Ergebnis: Die AS/400 antwortet, somit war unsere DNS-Konfiguration erfolgreich.

Jetzt prüfen wir noch einmal nur mit dem Hostnamen der AS/400:

2. PING: mit Hostnamen
   ping eposas03



2. Erfolgreicher PING

Sie sehen auch hier: Die AS/400 antwortet, somit war auch hier unsere DNS-Konfiguration erfolgreich.

Als Nachtrag:
Arbeiten Sie mit mehreren Domänen, so können Sie dem Client sagen, welche Domänen er zuerst durchsuchen soll.

Domänensuffix

Dies geschieht, indem Sie in den DNS-Eigenschaften des Clients eine Suchreihenfolge für die Domänensuffixe festlegen.

Im angezeigten Dialog sehen Sie, dass die Domäne EPOSHMBH.DE zuerst nach in Frage kommenden Adressen durchsucht wird. Arbeiten Sie nur mit einer Domäne, so muss dieser Eintrag nicht erfolgen.